Integritetsskydds
myndigheten

Integritetsskyddsrapport 2020

- redovisning av utvecklingen på it-området när det gäller integritet och ny teknik

IMY rapport 2021:1



IMY. Integritetsskyddsrapport 2020.
Har du frågor om innehållet kontakta Integritetsskyddsmyndigheten,
telefon 08-657 61 00, e-post imy@imy.se,
eller besök www.imy.se

Innehåll

Förord



Sverige är ett av EU:s mest digitaliserade länder, med ambitionen att bli bäst i världen på att använda digitaliseringens möjligheter. Med hjälp av datadriven och digital innovation skapas nya tjänster och funktioner som ger värde för samhälle, miljö, företag och ökad livskvalitet för enskilda individer.

Samtidigt skapar de enorma mängder data som samlas hos privata och offentliga aktörer stora risker. Möjligheten att kartlägga individer, deras rörelsemönster, preferenser, umgänge, hälsa, ekonomi med mera skapar en utsatthet för den enskilde.

Regeringen gav under 2019 Datainspektionen i uppdrag att vart fjärde år redovisa utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik. Denna rapport utgör den första redovisningen enligt uppdraget. Eftersom Datainspektionen den 1 januari 2021 bytt namn lämnas rapporten i Integritetsskyddsmyndighetens (IMY:s) namn.

Regeringen är primär mottagare av rapporten, men har aviserat att rapporten också ska ligga till grund för en riksdagsskrivelse. Därmed är även riksdagens ledamöter en viktig målgrupp för redovisningen. Även andra beslutsfattare och dataskyddsombud med flera som arbetar praktiskt med dataskydd, informations- eller cybersäkerhet kan sannolikt ha behållning av olika delar i rapporten.

Vår ambition är att rapporten ska bidra till utvecklingen av Sveriges integritetsskyddspolitik. Att en sådan politik behöver utvecklas är vår viktigaste rekommendation i vår första redovisning till regeringen. Med den snabba teknikutvecklingen inom till exempel Internet of things, artificiell intelligens och en ökad insamling av biometriska uppgifter riskerar Sverige annars att bygga in sig i en storskalig insamling och användning av data som är oetisk, olaglig eller på ett allvarligt sätt inskränker kommande generationers mänskliga rättigheter.

Genomförd tillsyn och granskningar visar att många organisationer fortfarande har grundläggande brister i sitt dataskyddsarbete. Det medför att gapet mellan teknikutvecklingen och integritets- och dataskyddet riskerar att kontinuerligt öka. För en hållbar och integritetsvänlig digitalisering behöver nu konkreta integritetsskyddspolitiska mål och åtgärder formuleras, vilket jag hoppas rapporten kan bidra till.

Lena Lindgren Schelin

Generaldirektör Integritetsskyddsmyndigheten (IMY)

1. Sammanfattning, slutsatser och rekommendationer

Hur kan utvecklingen på it-området förstås när det gäller frågor som rör integritet och ny teknik? Vad har påverkat den personliga integriteten mest de senaste åren, hur bra är integritetsskyddet idag och vad kommer ha störst betydelse om vi blickar några år framåt? I detta inledande avsnitt sammanfattar vi rapportens olika delar. Efter sammanfattningen följer centrala slutsatser och IMY:s rekommendationer.



1.1 Sammanfattning

Vi befinner oss i den fjärde industriella revolutionen. Kärnan i den pågående teknikutvecklingen handlar om att förmågan att skapa, använda och dela data utvecklats. Ny teknik har på kort tid gjort det enklare och billigare att samla in och med bland annat hjälp av artificiell intelligens, AI, bearbeta och analysera stora mängder data.

Inom en rad områden ger datadriven innovation hopp om att bättre kunna möta samtidens stora globala och nationella utmaningar och skapa ett bättre samhälle – nu och för kommande generationer. Genom nya sätt att resa, bo, konsumera, kommunicera och leva kan vi bli bättre på att tillvarata och bevara jordens resurser på ett hållbart sätt. Digitalt drivna innovationer kring vägar, transporter och varuflöden kan till bidra till att minska klimat- och miljöpåverkan. Samhällsplaneringen blir mer ändamålsenlig när funktioner som vatten- och energiförsörjning och annan infrastruktur kan dimensioneras utifrån stora mängder data. Även livsmedelsproduktion kan optimeras, kvalitet och effektivitet i välfärden utvecklas och medicinsk forskning på stora mängder patientdata användas för att utveckla botemedel och behandlingar mot svåra sjukdomar. Att smittspårning kan utgöra ytterligare ett tillämpningsområde har tydliggjorts under den pågående pandemin.

Tillgången till stora datamängder och möjligheterna att analysera dem innebär stora möjligheter. Samtidigt innebär den ökande insamlingen av data om vårt beteende och rörelsemönster, dels på nätet, dels i den fysiska världen, ofrånkomligen risker ur ett integritetsskyddsperspektiv. Kraftfull teknik för att samla in data ger en mängd aktörer tillgång till en mer eller mindre fullständig bild av våra liv, våra intressen, våra kontakter, vår hälsa och våra rörelsemönster, vanor och beteenden.

Det finns ingen vedertagen definition av personlig integritet, men i de statliga utredningar som gjorts på området under de senaste decennierna återfinns en tydlig röd tråd. Även om någon fast definition inte slås fast i denna rapport utgår vi från en förståelse av personlig integritet som den enskilde individens rätt till privatliv och möjlighet till självbestämmande i det digitala samhället. Med utgångspunkt i IMY:s uppdrag ligger fokus här enbart på personlig integritet i bemärkelsen skyddet av personuppgifter, även om integritetsbegreppet i vidare mening också kan omfatta skydd mot andra typer av godtyckliga intrång.

Kärnan i rätten till privatliv handlar här om rättigheten att även i digitala miljöer kunna ha privata förehavanden och kommunicera förtroligt utan att bli kartlagd, spårad eller övervakad – vare sig av myndigheter eller av globala storföretag. I möjligheten till självbestämmande ingår att själv kunna kontrollera vem som använder digitala uppgifter som rör en själv och för vilka syften. Ingen av dessa rättigheter är absolut, vilket sannolikt är en förklaring till att lagstiftaren inte tydligt har definierat begreppet personlig integritet.

Rätten till privatliv är en grundläggande mänsklig rättighet, men också i hög grad en demokratifråga eftersom det är svårt att utöva andra grundläggande rättigheter som åsikts-, yttrande- och organisationsfrihet om vi inte vet om vi övervakas och av vem. Ett gott integritetsskydd har också stor betydelse för individers säkerhet. I synnerhet om personuppgifter hamnar i orätta händer kan det innebära konkreta risker för den enskilde. Ett gott integritetsskydd har betydelse också för Sveriges säkerhet. Omfattande läckage av uppgifter till främmande makt eller andra antagonistiska aktörer kan utnyttjas som ett geopolitiskt maktmedel och påverka Sveriges säkerhetsskydd.

1.1.1 Ambitiös digitaliseringspolitik såväl på EU-nivå som nationellt

Inom EU har viktiga initiativ tagits de senaste åren för att möta den snabba tekniska utvecklingen och ökande insamlingen och delningen av personuppgifter. Den viktigaste integritetsstärkande reformen är att dataskyddsförordningen, GDPR, infördes som lag i EU:s medlemsstater och ett direktiv på det brottsbekämpande området, som implementerades i svensk rätt genom brottsdatalagen och brottsdataförordningen, trädde i kraft under 2018.

Dataskyddsförordningen innehåller förstärkta rättigheter för enskilda individer, som ska kunna utöva insyn och ha kontroll över sina personuppgifter. Samtidigt innebär förordningen på en rad områden skärpta skyldigheter för verksamheter som hanterar personuppgifter. Skyldigheterna för verksamheterna sammanfattas i förordningens sex grundläggande principer om laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, riktighet, lagringsminimering samt integritet och konfidentialitet. Är inte de grundläggande principerna beaktade, eller om rättslig grund saknas, kan man utgå från att personuppgiftsbehandlingen inte är laglig. Förordningen innehåller också helt nya verktyg för korrigerande befogenheter, bland annat kraftfulla sanktionsavgifter.

Genom dataskyddsförordningen inrättades också den Europeiska dataskyddsstyrelsen, EDPB. Styrelsen beslutar om yttranden och vägledningar men har även mandat att fatta beslut i gränsöverskridande ärenden. Styrelsens mandat är omfattande, både på policynivå och operativt. I praktiken har en stor del av den nationella suveräniteten när det kommer till tolkning och tillämpning av dataskyddsregleringen samt praxisbildning överlämnats till EDPB.

I sin tvåårsutvärdering av dataskyddsförordningen bedömde EU-kommissionen att reformen uppfyllt det övergripande målet att stärka skyddet av den enskildes rätt till skydd av personuppgifter. Samtidigt understryker kommissionen att det behövs ökade ansträngningar, bland annat för att medborgarnas kontroll över deras egen data ska bli reell. Att stärka enskildas rättigheter behöver bland annat ske när det gäller tillgång till och användning av data, till exempel rätten till information och rätten till radering av data. Kommissionen menade också att harmoniseringen mellan länderna har ökat, men att det fortfarande behövs en mer enhetlig tillämpning i hela unionen.

EU har höga ambitioner på digitaliseringsområdet för de kommande åren. I februari 2020 presenterade EU-kommissionen tre strategiska dokument som anger inriktningen för EU:s digitala framtid: en övergripande digitaliseringsstrategi, en datastrategi och en vitbok om AI. Genomgående innehåller dokumenten en kombination av å ena sidan offensiva satsningar och investeringar för att bli världsledande på att dra nytta av teknikens fördelar, å andra sidan åtgärder för att fortsätta stärka och säkerställa medborgarnas rättigheter. Konkreta åtgärder för att höja säkerheten och skydda enskilda individers fri- och rättigheter presenterades också i den nya cybersäkerhetsstrategi som kommissionen lade fram i december 2020.

Datastrategin innehåller åtgärder för att utveckla ett rättsligt ramverk kring dataanvändning, ökade investeringar för att stärka kapaciteten att använda data, åtgärder för att stärka individers möjlighet att kontrollera deras egna data samt åtgärder för att möjliggöra gemensamma europeiska datautrymmen.

Vitboken om AI anger målsättningen att EU ska bli världsledande på AI-teknik, samtidigt som medborgarnas rättigheter säkras. Offensiva satsningar och kraftigt ökade investeringar ska kombineras med ett intensifierat arbete för att tydliggöra ett etiskt och rättsligt ramverk. Som ett första steg i att utveckla det rättsliga ramverket har ett antal etiska principer för användning av AI utarbetats.

Även på nationell nivå har digitaliseringspolitiken fått en tydlig prioritering de senaste åren, bland annat genom framtagandet av en nationell digitaliseringsstrategi och en nationell inriktning för AI. Sverige ska enligt regeringens digitala strategi vara bäst i världen på att ta tillvara digitaliseringens möjligheter. Genom delmålet digital trygghet har Sveriges digitaliseringsstrategi en liknande ansats som EU-kommissionens, nämligen att satsningar på innovation och datadriven utveckling behöver kompletteras med åtgärder för att möta de risker som uppstår när allt fler saker kopplas upp och vi tillbringar allt mer av vår tid i digitala miljöer.

Den nationella inriktningen för AI anger att Sverige ska vara ledande i att ta tillvara möjligheterna som användning av AI kan ge. I den nationella inriktningen konstaterar regeringen att hur olika aktörer förmår omsätta dataskyddsförordningen i sina respektive verksamheter kommer att ha betydelse för hur väl Sverige förmår ta hand om potentialen och hantera riskerna med AI.

Sedan 2018 har regeringen gett olika myndigheter en rad särskilda uppdrag för att främja Sveriges förmåga att använda AI, skapa och använda öppna data och fortsätta digitalisera den offentliga sektorn. Även avseende informations- och cybersäkerhet har en nationell strategi utarbetats och en rad åtgärder vidtagits. Ännu saknas dock mer konkreta politiska mål och åtgärder som bygger vidare på dataskyddsreformens intentioner och ger en tydlig inriktning för utvecklingen av Sveriges arbete med integritets- och dataskydd.

1.1.2 Sexton teknikområden som påverkar den personliga integriteten

I rapporten beskriver vi sexton olika teknikutvecklingsområden som tillsammans bidrar till utveckling och Sveriges förmåga att ta tillvara digitaliseringens möjligheter, men samtidigt haft stor betydelse för den personliga integriteten. Vi bedömer att flera av områdena också kommer ha en avgörande påverkan på integritetsskyddet under de kommande åren.

Teknikområdena hänger nära samman, inte minst eftersom utveckling inom ett område många gånger har förstärkt och snabbat upp utvecklingen inom andra områden. Vi har dock i rapporten valt att dela upp teknikområdena i teknik för att samla in, bearbeta och analysera, lagra, transportera, säkra och förstöra data.

Många av de teknikutvecklingsområden som beskrivs i rapporten utvecklas exponentiellt, vilket förenklat innebär att kapaciteten fördubblas ungefär vartannat år. Innovation möjliggör nya innovationer och skapar ett slags ”ränta på ränta-effekt” som accelererar tempot i teknikutvecklingen. Till följd av den exponentiella utvecklingen beräknas de kommande 100 åren motsvara 20 000 år av teknikutveckling.

1.1.2.1 Ny teknik för att samla in data

Det övergripande teknikutvecklingsområde som sannolikt påverkat den personliga integriteten allra mest de senaste åren är den ökande insamlingen av data om vårt beteende och rörelsemönster, dels på nätet, dels i den fysiska världen. Ekonomiska och affärsmässiga intressen har varit en viktig drivkraft för utvecklingen då det finns goda möjligheter att tjäna pengar på data. Ny teknik för att samla in data ger en mängd aktörer tillgång till en fullständig bild av våra liv, våra intressen, våra kontakter, vår hälsa, våra rörelsemönster, vanor och beteenden.

Risker för den enskilde individen med den ökande datainsamlingen handlar bland annat om att det blir allt svårare att upptäcka, kontrollera eller välja bort att data om oss samlas in. Det faktum att uppgifter delas mellan olika aktörer på ett sätt som ofta är svåröverblickbart både för den enskilde individen och för verksamheterna som delar data gör integritetsriskerna större. Det finns också en risk för ändamålsglidning, det vill säga att uppgifterna används för andra ändamål än de ursprungligen samlats in för.

Centralt i utvecklingen av teknik för att samla in data är att *sensorer och sändare* utvecklas mot att bli allt mindre men samtidigt mer kraftfulla. Som exempel kan nämnas kroppsnära teknik som pulsklockor och träningsarmband och geospatial teknik för positioneringsdata.

Ytterligare ett område där teknikutvecklingen gått snabbt framåt de senaste åren handlar om *nya former för interaktion mellan människa och dator*. På kort tid har röststyrningsteknik fått ett brett genomslag och spridits från mobiltelefoner och datorer till bland annat bilar, klockor, hörlurar och olika smarta prylar i hemmet som till exempel TV-apparater. Även teknik för avläsning av fingeravtryck och ansiktsigenkänning utvecklas snabbt.

Utvecklingen inom *Internet of things, IoT*, utgör ett särskilt riskområde ur ett integritetsperspektiv. IoT avser apparater, maskiner och fordon som har inbyggd teknik och internetuppkoppling, men typiskt sett inte ses som datorer. Det kan vara vardagsföremål som vitvaror, termostater, belysning, TV-apparater, elektroniska lås och larm, kläder eller bilar, men också utrustning i industri, infrastruktur eller vården. Utvecklingen går mot att IoT används inom allt fler samhällsområden och på allt fler geografiska platser för att samla in data. En stor andel IoT-enheter har visat sig ha bristande säkerhet. Forskare har till exempel visat hur man kan ta kontroll över en modern bil via ett trådlöst nät, eller via fjärrstyrning manipulera en pacemaker eller insulinpump.

Med teknik för *webbskrapning* som kombineras med artificiell intelligens, AI, är det förhållandevis enkelt att samla in och bearbeta mycket stora informationsmängder från nätet, exempelvis från sociala medier. Kännetecknande är ofta att informationsmängderna blir så stora att det blir oöverblickbart och kräver AI-teknik för bearbetning.

En särskild typ av datainsamling som i ökande utsträckning används inom allt fler samhällsområden handlar om insamling av *biometriska uppgifter*. Biometri innebär att mäta kroppens egenskaper (till exempel hand- eller fingeravtryck, mönster i ögats iris, ansikts- eller kroppsform och röstavtryck) eller individers beteenden (till exempel gångstil, rörelse- och talmönster, handstil, ansiktsuttryck och sömnmönster) för att verifiera, autentisera eller identifiera individer. Användning av biometriska uppgifter kan skapa ökad bekvämlighet, snabbhet och säkerhet. Samtidigt medför den ökande användningen av biometriska uppgifter betydande integritetsrisker. En av de främsta riskerna handlar om att biometriska data (till skillnad från till exempel lösenord eller passerkort) inte kan bytas ut om uppgifterna skulle hamna i orätta händer. De biometriska uppgifterna är beständiga, vilket gör en integritetsförlust svår att reparera.

1.1.2.2 Ny teknik för att bearbeta och analysera data

De ökade möjligheterna att samla in data skulle i praktiken vara värdelösa om inte tekniken för att bearbeta och använda uppgifterna också tagit stora utvecklingssprång. Utvecklingen av *artificiell intelligens (AI)* har därför haft avgörande påverkan på den personliga integriteten under de senaste åren. De möjliga nyttorna med AI är stora och den outnyttjade potentialen fortfarande stor. I dagsläget uppges ungefär fem procent av svenska företag och tio procent i offentlig sektor använda AI i sina verksamheter.

Samtidigt innebär AI integritetsrisker för den enskilde i form av bland annat bristande transparens, diskriminering, försvårat ansvarsutkrävande, missbruk och fientlig användning. Särskilda risker finns vid automatiserade processer i beslutsfattande, när ett beslut kan få stora konsekvenser för den enskilde.

Ett av de områden där den omfattande AI-bearbetningen av stora datamängder blir allra mest uppenbar för många människor är den *digitala annonsmarknaden*. De komplexa och icke transparenta processerna som kan inkludera hundratals aktörer gör det i praktiken omöjligt för den enskilde att utnyttja sina rättigheter, till exempel att få information raderad. Affärsmodellerna gör det i praktiken också mycket svårt för företagen att ha kontroll och uppfylla sina skyldigheter när det gäller enskildas rättigheter. Såväl norska som brittiska myndigheter har i färska analyser kommit till slutsatsen att stora delar av den digitala annonsmarknaden systematiskt bryter mot dataskyddslagstiftningen.

1.1.2.3 Ny teknik för att lagra, säkra och transportera data

I takt med att insamlingen och bearbetningen av data blir allt mer omfattande och sofistikerad växer också kraven på lagringskapacitet. Den teknik som hittills svarat väl mot de stora behoven av lagringskapacitet är avancerad *molnlagring*. En utmaning med bearbetning eller lagring i molntjänster är att marknaden för molntjänster idag domineras av amerikanska aktörer vilket kan medföra att lagringen, efter EU-domstolens avgörande i juli 2020 i det så kallade Schrems II-målet, inte är laglig.

En konsekvens av att lagringskapaciteten har ökat och att kostnaderna för lagring minskat är att incitamenten att förstöra data minskat. Tidigare förstördes gammal data för att hushålla med lagringsutrymme och göra plats för ny. Inom övriga områden har teknikutveckling inom ett område drivit på utvecklingen inom andra områden. När det gäller teknik för att förstöra data har utvecklingen snarast gått i motsats riktning, och väsentligt större fokus har lagts på ny *teknik för att återskapa raderad data*, än teknik för att permanent förstöra den.

Ett utvecklingsområde som kan innebära fördelar ur ett integritetsperspektiv handlar om var data bearbetas – i centrala datacentra och serverhallar eller lokalt. Teknik för *edge computing* medför att bearbetning av data nu allt oftare kan ske lokalt, i uppkopplade enheter med låg kapacitet eller i lokala servrar. Detta innebär att data i mindre utsträckning behöver transporteras och delas, vilket kan skapa bättre kontroll. Med utvecklingen inom IoT ökar också behovet av lagring och säkring direkt i enheterna utan att behöva transportera data i nätet. Sådan teknik benämns ofta *edge storage* och *edge security*, det vill säga att personuppgifter kan lagras och säkras direkt i de lokala enheter där de samlas in, exempelvis i en privatpersons smarta mobiltelefon.

En ökad insamling och förmåga att bearbeta och använda data ställer också helt nya krav på infrastruktur och teknik för att transportera stora datamängder. *5G* är nästa generation av mobila nätverk med extremt hög kapacitet för att transportera data. För EU-kommissionen är utvecklingen mot 6G redan en prioriterad fråga. Ett centralt användningsområde för 5G och 6G kommer att vara IoT med till exempel uppkopplade enheter i industrin och i smarta städer. En integritetsrisk kopplat till 5G handlar om att geografisk positionering kommer vara möjligt med mycket med större precision än idag. Ett annat exempel på integritetsrisker som 5G medför är kopplat till en ökad insamling av högupplöst bildmaterial. Möjligheten att utan fördröjning överföra stora mängder högupplösta bilder kommer sannolikt utgöra en pådrivande faktor för en ökad direkt och indirekt insamling av biometrisk data.

Andra former av *digital kommunikationsteknik* som utvecklas tar sikte på kommunikation på nära avstånd, till exempel mellan enheter i ett och samma rum eller i chip som kan monteras i prislappar.

Utvecklingen med fler uppkopplade enheter och ökad molnlagring har ökat antalet möjliga vägar för angripare att komma åt system, nät, datorer, enheter eller servrar. En ökad hotbild har drivit på utvecklingen av *ny säkerhetsteknik* som till exempel automatiserade säkerhetslösningar baserade på AI. Även nya och fler lättanvända *krypteringslösningar* har utvecklats de senaste åren. Rätt använd kan den nya tekniken stärka integritetsskyddet.

1.1.3 Hur bra är integritetsskyddet idag?

I rapporten görs ett antal övergripande iakttagelser utifrån Integritetsskyddsmyndighetens, IMY:s, olika verksamhetsområden efter de första drygt två och ett halvt åren sedan dataskyddsreformen genomfördes.

Ett år efter att dataskyddsförordningen trädde i kraft genomförde IMY en undersökning av hur långt dataskyddsarbetet kommit i svenska företag, myndigheter och andra organisationer. Resultatet visade att de flesta fått grundläggande strukturer och rutiner på plats, men att det fortfarande i många verksamheter saknades ett systematiskt och kontinuerligt arbete. Branscher som hade större utmaningar var generellt kommuner och regioner, transportsektorn, hotell- och restaurangbranschen samt småbolag med mindre än 10 anställda. Genomgående beskrev företag, myndigheter och andra organisationer att de största utmaningarna i dataskyddsarbetet handlade om att få till fungerande processer i det löpande arbetet och att tolka regelverket.

IMY:s övergripande bedömning är att det nu, två och ett halvt år efter att dataskyddsförordningen trädde i kraft, fortfarande i många verksamheter finns omfattande brister som rör grundläggande skyldigheter i dataskyddsarbetet. De närmare 500 sanktionsavgifter som hittills utfärdats inom EU visar att de vanligaste överträdelserna handlar om att de grundläggande principerna inte följs, att rättslig grund för behandlingen saknas, att enskildas rättigheter inte hanteras som de ska eller att säkerhetsåtgärderna varit otillräckliga.

Även de cirka 7 500 klagomål som skickats in till IMY ger bilden av att det finns återkommande brister kring rättslig grund, enskildas rättigheter och säkerhetsåtgärder. Ungefär en fjärdedel av alla klagomål handlar om de rättigheter som förordningen ger medborgarna. Den vanligaste rättigheten som berörs i klagomålen är rätten till radering och därefter rätten till information. Andra vanliga klagomål handlar om bristande säkerhet eller att medborgare ifrågasätter om verksamheterna har rätt att hantera personuppgifter på det sätt de gör, det vill säga om det finns rättslig grund.

Omkring 11 000 personuppgiftsincidenter har hittills anmälts i Sverige sedan dataskyddsförordningen trädde i kraft. En viktig slutsats från anmälningarna är att många incidenter orsakas av den mänskliga faktorn. Det accentuerar behovet av att relevanta it-säkerhetsåtgärder kompletteras med organisatoriska åtgärder i form av till exempel löpande utbildning och andra åtgärder för att öka kunskapen och medvetenheten hos medarbetarna.

Bland de förhandssamråd som inkommit till IMY återfinns flera där verksamheten önskar använda teknik för ansiktsigenkänning och biometriska uppgifter. Totalt sett är det dock få verksamheter som begärt förhandssamråd, vilket tyder på att åtgärden att genomföra konsekvensbedömningar behöver öka.

En av de mest centrala och mest frekvent återkommande synpunkterna i de remisser IMY svarat på under de senaste åren har rört behovet av att tidigt i lagstiftningsarbetet göra en ingående integritetsskyddsanalys. Ju mer genomarbetad nationell lagstiftning som kompletterar dataskyddsförordningen är, desto enklare blir det för företag, myndigheter och andra organisationer att tolka och tillämpa dataskyddsreglerna. Vi får då också en lagstiftning som är homogen och heltäckande och ger verksamheterna det stöd de behöver för sin personuppgiftshantering.

1.1.4 Exempel på svensk forskning om integritet och dataskydd

I rapporten ges några exempel på färsk eller pågående svensk forskning inom integritet och dataskydd. Forskningen har identifierat flera riskområden när det gäller personlig integritet, bland annat när det gäller AI. Identifierade problemområden med AI handlar bland annat om risken för partisk AI och missbruk men också att säkerställa ansvarsfrågor och transparens.

Inom akademin finns också ett antal pågående projekt och initiativ som på olika sätt syftar till att höja integritetsskyddet. Ett område som flera lärosäten forskar om är transparens och nya verktyg för att öka användarnas kunskap om och kontroll över vilka personuppgifter som samlas in och används – av vem, på vilket sätt samt eventuella konsekvenser av användningen. Integritet vid användning av appar har stått i fokus i flera studier. När det gäller inbyggt dataskydd och dataskydd som standard har forskare arbetat fram onlineutbildningar i dataskydd, bland annat en med särskilt inriktning mot inbyggt dataskydd. Forskning pågår också för att utveckla säkra molntjänster och höja säkerheten i IoT.

1.2 Slutsatser

Det är en sliten formulering att teknikutvecklingen går snabbt. Likväl är det – i beskrivningen av utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik – en helt avgörande utgångspunkt som behöver ligga till grund för alla efterföljande, mer detaljerade slutsatser och rekommendationer.

Det finns en mängd svåra och angelägna dagsaktuella frågor i dataskyddsarbetet. Många organisationer uppvisar fortfarande brister i de grundläggande skyldigheter som införts genom dataskyddsförordningen. Att tolka och tillämpa regelverket utmanar företag och andra verksamheter, dataskyddsombud och andra som arbetar praktiskt med dataskydd samt dataskyddsmyndigheterna runt om i Europa. Några exempel på utmaningar som varit särskilt aktuella under 2020 är hur tredjelandsöverföringar (det vill säga överföring av personuppgifter till länder utanför EU/EES) ska hanteras efter EU-domstolens avgörande i Schrems II-målet och olika frågor som aktualiserats med anledning av den pågående Covid 19-pandemin.

Med exponentiell utveckling följer också – om inte riskreducerande åtgärder vidtas – exponentiellt ökande integritetsrisker. I exponentiella utvecklingsprocesser finns alltid en risk att vi tillmäter kortsiktiga frågor oproportionerligt stor betydelse och att de steg och mått som tas för att motverka risker är ”linjära”.

Mot denna bakgrund är ambitionen här inte primärt att beskriva frågor som i nuläget står högt på många dataskyddspraktikers agenda utan att peka på större och mer övergripande slutsatser och iakttagelser. Dessa ligger sedan till grund för de rekommendationer som rapporten utmynnar i.

1.2.1 De flesta känner till att allt vi gör på nätet lämnar spår – men ny teknik tar datainsamlingen på nätet till nya dimensioner

Att så gott som allt vi gör online lämnar spår och kan kartläggas förvånar knappast någon längre. För många människor i västvärlden är den digitala annonsmarknaden sannolikt det område där omfattningen (och hastigheten) i den datainsamling som idag sker på nätet blir som mest uppenbar. Utvecklingen av AI har varit en viktig möjliggörare. Ekonomiska drivkrafter har också spelat stor roll och möjligheterna att tjäna pengar på data har lett till framväxten av nya affärsmodeller som i stor utsträckning bygger på en ökad insamling och bearbetning av data. Vi har vant oss vid att en viss sökning på internet, ett besök på en viss webbsida eller nedladdning av en viss app strax efteråt resulterar i att annonser på samma tema syns i våra digitala flöden. Även om personaliserad marknadsföring på nätet för en del skapar en olustkänsla, har det blivit en del av vår digitala vardag.

Samtidigt är det viktigt att understryka, att även om vi vant oss vid att vara föremål för omfattande spårning på nätet betyder det inte att databehandlingen är laglig. Tvärtom har flera europeiska myndigheter kommit till slutsatsen att en stor del av den handel med data som sker i den digitala annonsindustrin är problematisk. Flera myndigheter, såväl i Sverige som i andra EU-länder, har i granskningar av den digitala annonsindustrin visat på det stora antalet aktörer som våra personuppgifter sprids till. Ett besök på en webbplats eller nedladdning av en app leder många gånger till att våra personuppgifter delas med mellan 10 och 30 andra företag utan att vi har någon affärsmässig relation med dem.

Såväl norska som brittiska myndigheter har i skarpa uttalanden klassat stora delar av den digitala annonsindustrin som illegal. Den brittiska dataskyddsmyndigheten ICO konstaterar att datahantering som strider mot dataskyddsreglerna genomsyrar hela branschen. Tre problemområden pekas ut särskilt; brist på transparens, avsaknad av rättslig grund för att behandla uppgifterna och bristande säkerhet. Omfattningen av skapandet och delandet av konsumentprofiler är oproportionerlig, inkräktande och oriktig – särskilt som många användare är omedvetna om att processerna sker. Komplexiteten och de många aktörerna gör det svårt även för verksamheterna själva att fullt ut överblicka vem som tar del av vilken data. Att säkerställa tillräckliga säkerhetsåtgärder är därmed problematiskt, särskilt när personuppgiftsbehandlingen involverar känsliga eller särskilt integritetskänsliga personuppgifter.

Det finns tydliga tecken på att negativa konsekvenser av den omfattande datainsamlingen som sker på nätet blivit en allt viktigare fråga för människor i Sverige under de senaste åren. Allt fler känner oro för hur deras personuppgifter hanteras och allt fler vidtar åtgärder för att skydda sina personuppgifter, eller avstår helt från att använda digitala tjänster som upplevs som osäkra. Ändå är magnituden och de potentiella konsekvenserna av hittills genomförd, men framför allt pågående och kommande, datainsamling svår att kontrollera och överblicka.

Ett start-upbolag som erbjuder en app-lösning till brottsbekämpande aktörer är ett tydligt exempel på hur ny teknik tar datainsamlingen på nätet till nya nivåer. Företaget har med webbskrapningsteknik byggt upp en databas med tre miljarder ansiktsbilder som hämtats från bland annat sociala medier. Med hjälp av AI och ansiktsigenkänningsteknik är det möjligt att ta en bild av en person, matcha den mot databasen och få veta vem personen är och få tillgång till all information som finns tillgänglig på nätet om personen i fråga.

Sammanfattningsvis har utvecklingen av AI under de senaste åren bidragit till en kraftigt ökad insamling av data om vårt beteende på nätet som i grunden påverkat den personliga integriteten. Att vi vant oss vid att vara föremål för omfattande spårning på nätet är inte synonymt med att den omfattande insamlingen och bearbetningen av data som sker är laglig.

Ur den enskilda individens perspektiv är ett centralt problem att möjligheterna att med AI-teknik bearbeta och samköra stora mängder data gör att information som ursprungligen inte är särskilt känslig – kanske inte ens utgör personuppgifter – i kombination med andra datamängder kan ändra karaktär och bli väldigt integritetskränkande. Det blir därmed allt svårare för enskilda att själva värdera känsligheten i en viss information.

Genom allt större möjligheter att indirekt identifiera individer i stora datamängder utökas också integritetsskyddsområdet. Etiska frågor om personlig integritet och praktisk tillämpning av dataskyddsregelverken kan därför under kommande år behöva beaktas även på områden och i frågor som vid första anblick inte alls handlar om behandling av personuppgifter.

Ett annat dilemma är att bulken av all information som samlas in är information som finns öppet tillgänglig på nätet, inte sällan uppgifter som vi själva offentliggjort. I mindre mängder är uppgifterna ofta harmlösa, men när informationsmängderna ökar exponentiellt ökar också integritetsriskerna i samma takt. Slutligen ökar integritetsriskerna av det faktum att uppgifter delas mellan olika aktörer på ett sätt som ofta är svåröverblickbart för den enskilde individen.

De allvarligaste överträdelserna går sannolikt att stävja med en kombination av kraftfull självsanering i branschen, skärpt tillsyn och kompletterande regelverk. Grundläggande informationssäkerhetsåtgärder är också en viktig del av lösningen – med en höjd lägstanivå minskar risken för felaktig hantering som beror på den mänskliga faktorn. IMY:s bedömning är dock att problem med olaglig datainsamling på nätet kommer att utgöra ett bestående problem under lång tid framöver.

1.2.2 Med Internet of things flyttar spårningen på nätet ut i städer och hem

Med bland annat hjälp av kroppsnära teknik och geospatiala sändare har datainsamlingen kommit att allt oftare omfatta våra rörelsemönster och beteenden även i den fysiska världen. Till vilka adresser åker vi, hur ofta, hur länge stannar vi, vilka andra är där samtidigt? Utvecklingen ger en mängd aktörer tillgång till en fullständig bild av våra liv, våra intressen, våra kontakter, våra rörelsemönster, vanor och beteenden.

IMY:s bedömning är att Internet of things, IoT, är ett av de utvecklingsområden som kommer ha störst påverkan på den personliga integriteten under de kommande åren. Att utvecklingstakten är hög när det gäller IoT visar sig genom att det är inom det här området som antalet patentansökningar har ökat snabbast de senaste åren. Mellan 2016 och 2019 fyrdubblades antalet patentansökningar som rör IoT. Kombinationen av utveckling inom ”smarta städer” och ”smarta hem” gör att vi omges av allt mer högpresterande – och potentiellt integritetskränkande – teknik, såväl i det offentliga rummet som i våra hem.

Det riktigt breda genomslaget för IoT bedöms dock fortfarande ligga framför oss. Drygt hälften av den svenska befolkningen uppgav 2019 att de hade en uppkopplad sak i hemmet. När det gäller tillämpningar i industrin och smarta städer bedöms utrullningen av 5G (och 6G) komma ha stor betydelse för en intensifierad användning de närmaste åren.

Tack vare sensorer och sändare som tar mindre utrymme, men samtidigt är mer kraftfulla, har nya och förbättrade möjligheter skapats att samla in data i alla slags former i det fysiska rummet, i allt större volymer, i nya format, på nya platser och i nya sammanhang. Nya typer av sensorer och sändare kan tillsammans samla in data över ett mycket stort fysiskt område. De kan monteras fast på till exempel byggnader, men också kopplas till rörliga objekt som fordon eller drönare. Utvecklingen har kommit så långt att sensorer och sändare bedöms kunna krympa till storleken av ett dammkorn och kopplas ihop i nätverk av ”smart damm” som kan flyta med strömmar och vindar. Potentialen för utvecklingen har beskrivits som att multiplicera IoT miljoner gånger.

En av de största riskerna med detta är att många av de IoT-produkter som hittills utvecklats generellt har en låg säkerhetsnivå. En begränsande faktor i sammanhanget har sannolikt handlat om ekonomiska incitament – att bygga in ett adekvat skydd medför kostnader som kan upplevas som omotiverade så länge efterfrågan från konsumenterna inte är mer uttalad. På informations- och cybersäkerhetsområdet har flera svenska myndigheter pekat på att brister kring IoT medför risker ur ett säkerhetsskyddsperspektiv.

Ur ett integritetsskyddsperspektiv handlar riskerna som följer av IoT och nätverk av uppkopplade sensorer och sändare främst om att enskilda individer ofrånkomligen riskerar att fångas upp och övervakas, även om det inte är syftet med datainsamlingen. Cyberfysiska system inom industrin eller smarta städer kommer att utgöra komplexa nätverk av fysiska maskiner, robotsystem, automatiserade fordon, digitala plattformar som kontrolleras av människor i kombination med AI-baserad mjukvara.

När mängden data som kommuniceras mellan maskiner ökar kraftigt, finns en uppenbar risk att den indirekta datainsamlingen ökar i motsvarande utsträckning. Sensorer på byggnader eller bilar kan förväntas fånga upp även ”irrelevanta” data, till exempel bilder av personer som går över gatan. Samtidigt möjliggör 5G positionering och bildöverföring med mycket större precision och hastighet än tidigare nätverk. Under vissa omständigheter kommer det vara enkelt att identifiera enskilda individer, i synnerhet om datan samkörs med andra typer av uppgifter.

Risken är stor att frånvaron av transparens som idag genomsyrar den digitala annonsmarknaden och annan handel med data på nätet sprider sig även till den fysiska världen, till smarta hem och smarta städer. Kännetecknande är att det i praktiken är omöjligt för den enskilde att överblicka hur ens data behandlas och av vem, men också svårt för de ansvariga verksamheterna att ha full kontroll över data och ansvarsförhållanden. Även de brister som idag finns på nätet i form av omfattande personuppgiftsbehandling utan rättslig grund och med bristande säkerhet riskerar att följa med ut i den fysiska världen.

Sverige, och andra länder, kan komma att hamna i ett läge där vi först sent i pågående digitaliseringsvåg på allvar inser vidden av hur den personliga integriteten påverkas – eller kommer att påverkas – av den omfattande datainsamlingen. När funktioner som till exempel individualiserad uppvärmning eller avfallshantering från hushåll, nätverk av sensorer i ett alltmer automatiserat trafiknät eller ansiktsigenkänningsteknik i bilar för att upptäcka rattonykterhet väl har lanserats på bred front, kan det i praktiken vara omöjligt att återkalla eller begränsa en omfattande datainsamling även om den konstateras vara oproportionerlig, oriktig och integritetskränkande.

Erfarenheterna från hur datainsamlingen på nätet utvecklats visar hur kombinationen av ekonomiska incitament, den snabba framväxten av nya affärsmodeller och utfasande av tidigare lösningar gör att utvecklingen går framåt med sådan fart att politiken och lagstiftaren har svårt att hinna med. Att ett ändamålsenligt dataskydd byggs in redan från början i den cyberfysiska infrastruktur som nu växer fram är därför mycket angeläget.

När organisationer samverkar och delar data kan nya risker uppstå. Eftersom det är först i de aggregerade datamängderna som hela riskbilden framträder behöver arbetssätt utvecklas där organisationer gör konkreta risk- och konsekvensanalyser både tillsammans och var för sig. För att bygga en hållbar utveckling behöver organisationer redan från början bygga in dataskydd som standard och ta ansvar för säkerheten i produkterna, både vad gäller det enskilda bidraget och aggregerade konsekvenser av hur datan delas, förädlas och återanvänds i kommande led.

Sammanfattningsvis kan utvecklingen beskrivas som att den omfattande insamling av data som sker på nätet – som de flesta i någon mån känner till och som blivit en del av vår digitala vardag – nu flyttar ut i den fysiska världen där den blir än svårare att upptäcka, kontrollera och avskärma sig från. Om inte riskreducerande åtgärder vidtas är sannolikheten stor att de brister och risker som idag finns på nätet också kommer att genomsyra våra smarta hem och städer. En negativ utveckling med bristande integritetsskydd blir allt svårare att bromsa och läka i efterhand och medför också risker med avseende på informations- och cybersäkerhet.

1.2.3 Insamling av biometrisk data ökar

Parallellt med att IoT och utvecklade nät genom 5G är på väg att få ett bredare genomslag ökar insamlingen av biometriska uppgifter. Data om våra fysiska egenskaper – som exempelvis hand- och fingeravtryck, ansikts-, röst- och taligenkänning eller DNA – kompletteras i allt större utsträckning med beteendebaserade uppgifter som gångstil, rörelse- och talmönster, handstil, ansiktsuttryck och sömnmönster.

Användning av biometriska uppgifter kan bidra till ökad bekvämlighet, snabbhet och säkerhet inom en rad samhällsområden och blir allt vanligare bland annat inom offentlig förvaltning, bank- och finans samt hälso- och sjukvården. Ett konkret exempel är hur ny teknik för interaktion mellan människor och datorer på kort tid fått många mobiltelefonanvändare att överge säkerhetskoder till förmån för identifiering med fingeravtryck eller ansiktsigenkänning. Röststyrningen slår också igenom allt mer och de digitala assistenterna blir allt smartare.

För den enskilde individen finns dock en rad inneboende risker som handlar om att biometriska uppgifter kan manipuleras eller användas för andra syften, till exempel identitetsstöld, intrång, utpressning eller bedrägerier. Precis som för andra typer av data finns också en risk för ändamålsglidning, det vill säga att uppgifterna används för andra syften än de ursprungligen samlades in för. Biometriska uppgifter aktualiserar också särskilda risker kopplat till bristande transparens. Att utöva sina grundläggande rättigheter kan vara svårt om den enskilde individen inte förstår att en viss typ av uppgifter utgör personuppgifter – vilket för många sannolikt inte är uppenbart när det gäller teknik som bygger på vitt skilda biometriska egenskaper och beteenden och som nu utvecklas i snabb takt.

Ur ett integritetsskyddsperspektiv är den mest oroväckande egenskapen hos biometriska personuppgifter att de inte enkelt kan ändras eller ersättas om de går förlorade. Ett lösenord eller passerkort kan ersättas med ett nytt om det skulle gå förlorat. Om individen förlorar kontrollen över sina biometriska personuppgifter kan de däremot inte ersättas. Integritetsskadorna kan i värsta fall bli permanenta, vilket gör integritetsfrågor kring biometri särskilt angelägna.

1.2.4 Höga ambitioner när det gäller datadriven innovation behöver kombineras med kraftfulla åtgärder för att stärka integritet och säkerhet

Som beskrivits ovan har Sverige en ambitiös digitaliseringspolitik där en rad konkreta politiska initiativ vidtagits för att främja datadriven innovation. Genom bland annat ett antal uppdrag till olika myndigheter har regeringen verkat för att främja användningen av AI och användandet av data som strategisk resurs. Ett antal konkreta steg har också vidtagits för att främja digitaliseringen av offentlig sektor.

När det gäller åtgärder för att minska riskerna med digitaliseringen, hantera frågor om etik och säkerhet och säkerställa skyddet för enskildas rättigheter, har arbetet hittills inte fått lika konkreta former i Sverige. Viktiga satsningar har skett inom informations- och cybersäkerhetsområdena – områden som har många beröringspunkter med dataskydd – vilket är positivt. Däremot saknas konkreta mål och åtgärder i stor utsträckning för integritets- och dataskyddet.

Utvecklingsmässigt finns ett viktigt momentum nu, innan det bredare genombrottet skett för bland annat AI och IoT och insamlingen av biometriska uppgifter ökat ytterligare. Den snabba utvecklingen av den digitala annonsindustrin och handel med data på nätet visar att när en omfattande datainsamling väl implementerats i verksamhets- eller affärsmodellen är de ekonomiska kostnaderna höga och incitamenten ofta starka för att inte dra tillbaka dem. Den exponentiella utvecklingen behöver därför kombineras med konkreta och kraftfulla åtgärder för att nu säkerställa integriteteten och säkerhetsaspekterna i utvecklingen.

1.3 Rekommendationer

Givet den exponentiella teknikutvecklingen och för att nå regeringens vision om en hållbar digitalisering, är det angeläget att politiska åtgärder för att stärka datadriven utveckling, innovation och användningen av AI kompletteras med konkreta mål och åtgärder för att stärka skyddet för medborgarnas integritet. Särskilt angeläget är det att arbetet med att digitalisera den offentliga förvaltningen matchas med handfasta åtgärder för att värna enskilda medborgares rättigheter. Tappar medborgarna förtroendet för hur offentlig sektor hanterar deras data riskerar tilliten till samhället i stort att påverkas negativt.

Mot denna bakgrund lämnar IMY följande rekommendationer.

1.3.1 Sverige behöver en integritetsskyddspolitik

Den stora potentialen i den fjärde industriella revolutionen handlar om att förädla och använda data som strategisk resurs. Genom datadriven utveckling kan Sverige och EU bättre möta samhällsutmaningar till exempel i form av miljö- och klimatåtgärder och utveckla en mer kvalitativ och effektiv välfärd. De stora datamängderna skapar också tillväxt för företag och nya digitala produkter och tjänster skapar värde för medborgare. Regeringen har de senaste åren gjort ambitiösa satsningar för att främja användandet av öppna data, AI-tillämpning och datadriven innovation i såväl privat som offentlig sektor. Regeringen har också gjort flera satsningar inom informations- och cybersäkerhetsområdena, vilket är positivt.

Nu behöver dessa delar av politiken kompletteras med lika konkreta mål och åtgärder för att säkerställa att utvecklingen är hållbar ur ett integritetsperspektiv, att vi inte bygger in oss i en storskalig insamling och användning av data som är oetisk, olaglig eller på ett allvarligt sätt inskränker kommande generationers mänskliga rättigheter.

IMY:s bedömning är att *Sverige behöver en tydligare integritetsskyddspolitik*. Med detta menar vi ett väl definierat politikområde som konkretiserar mål och åtgärder för att i den pågående digitaliseringen säkerställa människors rätt till privatliv och rätten till självbestämmande i samband med behandling av personuppgifter.

En tydlig integritetsskyddspolitik behöver innehålla *konkreta mål och åtgärde*r. En *riskbaserad ansats* bör vara utgångspunkten för arbetet och det bör framgå av den politiska inriktningen hur Sverige avser att minska riskerna kring teknikutvecklingsområden som till exempel AI, IoT och biometri där integritetsriskerna är särskilt stora. Det kan möjligen också finnas anledning att särskilt utreda i vilken mån och på vilket sätt den offentliga förvaltningen bör nyttja denna typ av högriskteknik.

Även om integritets- och dataskyddsfrågor finns i alla samhällssektorer är det angeläget att ansvaret för integritetsskyddspolitiken har en tydlig hemvist inom regeringen och Regeringskansliet. Idag sker styrningen av IMY från Justitiedepartementet. Givet integritetsskyddsfrågornas starka inslag av mänskliga rättigheter och det praktiska dataskyddsarbetets stora inslag av rättsutveckling anser vi att det är en god ordning. För att inte gapet mellan teknik- och rättsutveckling ska öka ytterligare är det dock angeläget att utformningen av en integritetsskyddspolitik *integreras nära med andra politikområden, inte minst digitaliseringspolitiken*. De forum och strukturer som regeringen skapat för att driva digitaliseringspolitiken (som till exempel Digitaliseringsrådet) har därmed en roll att fylla även i utformningen av en integritetsskyddspolitik. Integritetsskyddspolitiken behöver också integreras i regeringens satsningar på informationssäkerhet- och cybersäkerhet. Sammantaget ställer en integritetsskyddspolitik krav på nära samverkan inom olika delar av Regeringskansliet, inte minst eftersom viktiga beröringspunkter också finns med till exempel konsument- och konkurrensfrågor.

1.3.1.1 Satsningar på integritetsskyddsteknik för tillväxt och konkurrenskraft

Lika mycket som exponentiella teknologier rymmer integritetsrisker är teknisk utveckling och innovation helt central för att utveckla morgondagens integritetsskydd. En central del av Sveriges integritetsskyddspolitik bör därför vara *offensiva investeringar för att stimulera forskning och utveckling av teknik som skyddar människors rätt till personlig integritet*.

De senaste åren har ett antal forskningsinitiativ startats med inriktning på integritetsskyddande teknik, men behoven är fortsatt stora. Det kan till exempel handla om att utveckla metoder för att göra träning och tillämpning av AI-algoritmer mer integritetsvänlig, att utveckla lösningar för att säkerställa att AI-teknik inte diskriminerar enskilda individer, att öka säkerheten i molntjänster och IoT samt fortsätta utveckla AI-baserad säkerhetsteknik eller anonymiserings- och krypteringslösningar. Tvärvetenskapliga ansatser behövs då utveckling, säkerhet, dataskydd och integritet ofta drivs av olika professioner och en långsiktigt hållbar utveckling kräver breda ansatser.

Dataskyddsförordningen har genom kraven på inbyggt dataskydd och dataskydd som standard lagt en god grund. Givet de enhetliga kraven i EU – och hur allt fler länder även utanför Europa anpassar sig till de europeiska dataskyddsreglerna – finns här goda tillväxtmöjligheter och en tydlig nisch där Sverige med sin starka it- och telekom-bransch har goda förutsättningar att bli världsledande. Genom satsningar på forskning och utveckling har regeringen möjlighet att stimulera innovativa tekniklösningar som skyddar mänskliga rättigheter och samtidigt bidrar till svensk konkurrenskraft.

1.3.1.2 Stärk enskilda individers rättigheter och möjlighet att kontrollera den egna datan

Regeringen har i budgetpropositionen för 2021 aviserat ambitionen att under 2021 ta fram en nationell datastrategi. Strategin är ett viktigt tillfälle för regeringen att *konkretisera mål och åtgärder för att stärka enskilda individers rättigheter och möjligheter att kontrollera den egna datan* – både i förhållande till myndigheter och i privat sektor. Det kan till exempel handla om åtgärder för att främja utvecklingen av appar eller andra verktyg som gör det enklare för människor att själva kontrollera och bestämma hur deras data används. Området är i sin linda, men i Sverige pågår forskning vid till exempel Karlstad, Lund och Luleå Tekniska universitet. Regeringen bör i framtagandet av datastrategin dra nytta av den forskning som finns på området i Sverige och kan också ta stöd i det arbete som kommissionen gör på området.

För att behålla medborgarnas tillit är det centralt hur offentlig sektor hanterar medborgarnas data. Regeringen uppdrog i september 2020 åt Arbetsförmedlingen, E-hälsomyndigheten, Myndigheten för digital förvaltning och Skatteverket att genomföra en omvärldsanalys och ta fram ett koncepttest som visar hur individens möjligheter till insyn och kontroll över de data om individen som finns hos offentlig sektor, och i förlängningen även de data om individen som finns hos privat sektor, kan öka. Uppdraget ska redovisas senast den 1 juni 2021. IMY ser positivt på uppdraget och bedömer att det sannolikt behöver åtföljas av fler uppföljande uppdrag eller utredningar för att stärka enskilda individers möjligheter att kontrollera den egna datan.

Som ett led i att stärka enskilda individers rättigheter kommer IMY under 2021 att utifrån inkomna klagomål börja återkoppla de brister som klagomålen gör gällande till de företag, myndigheter och andra organisationer som klagomålen riktar sig mot. Vi kommer också att inleda fler tillsyner än tidigare baserat på klagomål. Vår bedömning är att detta förändrade arbetssätt kan ge signaler om förbättringsbehov och bidra till lärande i såväl granskade som andra verksamheter. På det sättet verkar vi för ett tryggt informationssamhälle.

1.3.1.3 Integrera dataskydd i pågående arbete med att förstärka Sveriges informations- och cybersäkerhet

Både nationellt och på EU-nivå har en rad insatser vidtagits för att höja Sveriges informations- och cybersäkerhet. Samtidigt bedömer ansvariga myndigheter på området att det behövs kraftfulla åtgärder för att fortsätta höja grundnivån av informations- och cybersäkerhet i samhället. Dataskydd, informations- och cybersäkerhet – och i förekommande fall säkerhetsskydd – kräver i stor utsträckning samma typ av kontinuerligt och systematiskt arbete, där hot, sårbarheter och risker ur olika perspektiv analyseras löpande och ligger till grund för att utforma, genomföra och följa upp åtgärder. Tillsammans är de olika perspektiven länkar i en större kedja som minskar risker för människors säkerhet och grundläggande fri- och rättigheter och skyddar såväl företag och andra verksamheters tillgångar som samhällets funktionalitet och robusthet. Eftersom stora mängder uppgifter om andra länders medborgare kan vara ett reellt geopolitiskt maktmedel är ett effektivt dataskydd också en central komponent även i skyddet av Sveriges säkerhet.

IMY:s bedömning är att *integritetsskyddspolitiska mål och aktiviteter bör integreras med det nationella arbetet med informations- och cybersäkerhet*. Mer konkret kan detta ske till exempel genom att regeringen kompletterar den nationella strategin för samhällets informations- och cybersäkerhet med mål och åtgärder som avser dataskydd. I nästa steg bör även handlingsplanen som hör till strategin och uppdraget till de myndigheter som ansvarar för att genomföra handlingsplanen ses över. Det befintliga samarbetet mellan IMY, Myndigheten för samhällsskydd och beredskap, MSB, och övriga myndigheter som ansvarar för åtgärder i den nationella handlingsplanen bör också förstärkas.

Såväl Säkerhetspolisen som försvarsmyndigheter har uttalat att utvecklingen av 5G och IoT kommer att ha betydelse för svensk säkerhet under lång tid framöver. Säkerhetsskyddslagstiftningen har också uppdaterats för att omfatta fler både privata och offentliga verksamheter. Bland annat Försvarsberedningens rapporter och regeringens nationella säkerhetsstrategi betonar att hela samhället behöver engageras i arbetet med samhällets informations- och cybersäkerhet. Dilemmat är att det är många aktörer i samhället som inte omfattas av regelverken på området. Eftersom dataskyddsregleringen gäller för *alla* verksamheter som hanterar personuppgifter kan dataskyddsarbetet sägas utgöra en plattform för en stark informations- och cybersäkerhet i Sverige.

Det praktiska dataskyddsarbetet förutsätter att varje organisation har god kontroll på sina informationsmängder, gör systematiska risk- och konsekvensanalyser och vidtar löpande åtgärder för att höja säkerheten kring informationen. Ökar kvaliteten i dataskyddsarbetet förbättras därmed även Sveriges förmåga att stå emot riktade cyberangrepp och minska riskerna för olyckor eller handhavandefel. Skyddet för mänskliga rättigheter värnas samtidigt som Sveriges digitala suveränitet förstärks.

1.3.2 Vidta åtgärder för att främja fortsatt regelutveckling

Dataskyddsförordningen bygger på ett antal grundläggande principer och omfattar ny teknik i takt med att tekniken utvecklas. I sin tvåårsutvärdering av förordningen har EU-kommissionen pekat på en central utmaning som handlar om att klargöra hur de grundläggande principerna ska tillämpas på ny teknik, såsom AI, IoT eller ansiktsigenkänning. Den regulatoriska utvecklingen är i huvudsak EU-gemensam, varför det är *centralt att Sverige tar en aktiv roll i det EU- gemensamma arbetet*.

För IMY:s del kommer det även de närmaste åren att vara en prioriterad uppgift att ta en ledande roll i utformningen av för Sverige centrala vägledningar i EDPB. För regeringens del kan åtgärder för att främja en fortsatt regelutveckling handla till exempel om att söka koalitioner med andra medlemsstater vars uppfattning ligger nära Sveriges på teknikområden med särskilt stora integritetsrisker – till exempel AI, biometri och IoT – och bygga upp en pool av nationella specialister som kan nomineras när kommissionen eller EDPB formerar expertgrupper.

En central del i att främja den fortsatta regelutvecklingen handlar om att *säkerställa att ny lagstiftning är förenlig med dataskyddsregleringen*. Luckor eller motstridigheter i lagstiftningen riskerar annars att skapa situationer där företag och andra verksamheter i praktiken tvingas välja mellan att bryta mot olika regelverk eller inte har tydligt lagstöd för att utföra verksamhetskritiska personuppgiftsbehandlingar. Regeringen bör vid framtagande av utredningsdirektiv alltid överväga om det bör framgå särskilt att en integritetsanalys ska genomföras. För att underlätta för kommittéväsendet att säkerställa att lagförslag är förenliga med dataskyddsregelverket kommer IMY under 2021 att ta fram en uppdaterad vägledning för kommittéväsendet kring att genomföra integritetsanalyser. Vi föreslår att denna vägledning sedan införlivas i kommittéhandboken.

En tredje aspekt för att främja fortsatt regelutveckling handlar om att *öka kunskapen om dataskyddsregleringen hos Sveriges innovationsaktörer*, det vill säga organisationer, människor och nätverk som driver skapande, spridning och innovativ exploatering av ny teknik. Det kan handla om till exempel forskningsfinansiärer, inkubatorer, science parks och projekt inom strategiska innovationsprogram. Syftet är att öka förmågan att ansvarsfullt bedriva datadriven innovation och teknikutveckling. IMY, Vinnova och AI Sweden har under 2020 påbörjat ett samarbete för att utveckla strukturerade former för proaktiv vägledning i tidiga skeden av innovationsprojekt. Regeringen bör överväga att skapa förutsättningar för IMY och Vinnova att genomföra riktade insatser för att höja kunskapen hos privata och offentliga aktörer i det svenska innovationssystemet med avseende på integritets- och dataskyddsfrågor. Genom att skapa former som medger en dialog mellan IMY och innovationsaktörer tidigt i innovationsprocessen ökar också myndighetens kunskap om teknikutveckling och praktiska utmaningar och lösningar när dataskyddsregelverket appliceras på ny teknik, vilket gör att myndigheten kan ge mer riktat stöd och vägledning till fler aktörer.

I förlängningen bör regeringen *överväga att skapa förutsättningar för IMY att driva regulatorisk testverksamhet*. Inom flera länder i Europa pågår försöksverksamhet med regulatoriska testbäddar där dataskyddsmyndigheten ger en mer fördjupad vägledning till utvalda innovationsprojekt. Regeringen bör noga följa hur till exempel det norska försöket med en regulatorisk testbädd utvecklas.

1.3.3 Privata och offentliga verksamheter behöver fortsätta förbättra sitt grundläggande dataskyddsarbete

Inom ramen för en samlad integritetsskyddspolitik som föreslagits ovan bör regeringen *vidta åtgärder för att säkerställa att privata och offentliga verksamheter fortsätter att förbättra sitt grundläggande dataskyddsarbete*. Många företag och myndigheter driver ett ambitiöst dataskyddsarbete. Samtidigt visar de cirka 500 ärenden med sanktionsavgifter som hittills beslutats av tillsynsmyndigheterna inom EU att merparten av överträdelserna rör grundläggande skyldigheter. Data behandlas på ett sätt som strider mot dataskyddsförordningens grundläggande principer, utan rättslig grund eller med bristfälliga säkerhetsåtgärder. Sammanfattningsvis visar sanktionsavgifterna att lägstanivån i dataskyddsarbetet fortfarande behöver höjas. Dataskyddsförordningen anger flera verktyg för ett systematiskt dataskyddsarbete som hittills underutnyttjats, till exempel konsekvensbedömningar, förhandssamråd och uppförandekoder.

Regeringen bör *säkerställa uppföljning av hur arbetet med dataskydd utvecklas i den offentliga förvaltningen*. Precis som regeringen tidigare konstaterat gällande informations- och cybersäkerhet behöver företag och andra organisationer öka sin kompetens även om dataskydd. Alla typer av organisationer behöver arbeta systematiskt med dataskydd. Dataskyddsarbetet behöver integreras med informations- och cybersäkerhetsarbetet och gå från att vara en teknisk eller juridisk fråga till en strategisk verksamhetsfråga. Att offentlig sektor inte har en oproportionerlig övervakning av människor och systematiskt arbetar för att säkerställa ett gott integritetsskydd är särskilt viktigt för att behålla tilliten till digitala lösningar. Uppföljning av hur den offentliga förvaltningens arbete med dataskydd utvecklas skulle till exempel kunna ske inom ramen för den struktur för uppföljning av det systematiska informationssäkerhetsarbetet som MSB har regeringens uppdrag att ta fram, alternativt genom särskilda återrapporteringskrav i myndigheters regleringsbrev.

2. Inledning

För att den digitala utvecklingen ska vara hållbar behöver satsningar på datadriven innovation kombineras med kraftfulla insatser för att värna den personliga integriteten.

I rapportens inledande avsnitt belyser vi varför en ökad användning av data är viktig - men också hur personlig integritet kan förstås och vad det har för betydelse ur till exempel ett demokrati-, säkerhets- och hållbarhetsperspektiv.

Vi går också igenom vissa skillnader och likheter mellan dataskydd, informationssäkerhet, cybersäkerhet och säkerhetsskydd och varför det är viktigt att se de olika delarna som länkar i en större kedja.

I det inledande kapitlet beskrivs också rapportens syfte och målgrupp samt hur vi gått tillväga när vi tagit fram rapporten.



Sverige är ett av EU:s mest digitaliserade länder, med ambitionen att bli bäst i världen på att använda digitaliseringens möjligheter. Allt från demokrati, regional utveckling, handel och arbetsliv till sociala samspel påverkas i grunden av teknikutvecklingen. Med hjälp av datadriven och digital innovation skapas nya tjänster och funktioner som ger värde för samhälle, miljö, företag och ökad livskvalitet för enskilda individer.

Kärnan i Datainspektionens uppdrag har sedan myndigheten bildades 1973 varit att värna medborgarnas personliga integritet. Under 2018 förstärktes det rättsliga skyddet för den personliga integriteten genom EU:s generella dataskyddsförordning (dataskyddsförordningen, ofta kallad GDPR)[1]. Kompletterande lagstiftning trädde ikraft i form av dataskyddslagen[2] och annan nationell lagstiftning. Ett EU-direktiv på det brottsbekämpande området implementerades i Sverige genom brottsdatalagen (BdL) och brottsdataförordningen.[3] Sammantaget innebär de nya regelverken att det rättsliga skyddet för den personliga integriteten nu är starkare än någonsin tidigare.

Samtidigt medför teknikutvecklingen att även hot och risker för den personliga integriteten är mer omfattande, långtgående och potentiellt allvarligare än någonsin tidigare. Ständigt ökande mängder data samlas in hos privata och offentliga aktörer, ofta i praktiken utan att den enskilde individen kan överblicka hur datan används, av vem eller varför.

En del av Datainspektionens uppdrag har sedan länge handlat om att följa, analysera och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik.[4] Under 2019 beslutade regeringen om ett tillägg i myndighetens instruktion innebärande att en redovisning av utvecklingen på området ska lämnas till regeringen vart fjärde år.[5] Regeringen har därefter beslutat att Datainspektionen per den 1 januari 2021 byter namn till Integritetsskyddsmyndigheten.

Denna rapport utgör Integritetsskyddsmyndighetens (IMY:s) första redovisning av uppdraget att följa, analysera och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik. Genomgående används IMY i rapporten för att beskriva myndighetens uppdrag och kunskapsunderlag etcetera. Datainspektionen används vid hänvisning till rapporter som har levererats i Datainspektionen namn.

1. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

2. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen.

3. Brottsdatalagen (2018:1177), brottsdataförordningen (2018:1202).

4. Förordning (2007:975) med instruktion för Integritetsskyddsmyndigheten, 1 §.

5. Förordning (2019:555) om ändring i förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten. Den första redovisningen ska enligt regeringens beslut överlämnas till regeringen senast den 1 oktober 2020. Med anledning av bland annat namnbytet har Integritetsskyddsmyndigheten begärt förlängd tid för att lämna in rapporten till den 28 januari 2021, vilket regeringen beviljat.

2.1 Om rapporten

Under 2019 beslutade regeringen om ett tillägg i Datainspektionens (numera Integritetsskyddsmyndigheten, IMY) instruktion innebärande att en redovisning av utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik ska lämnas till regeringen vart fjärde år. Denna rapport utgör den första redovisningen enligt uppdraget.

Rapporten riktar sig i första hand till regeringen, riksdagen och andra policyskapande beslutsfattare.

Rapporten innehåller bland annat en beskrivning av ett antal teknikutvecklingsområden och genomförda åtgärder som påverkar den personliga integriteten. Syftet är att ge underlag för prioriteringar och bidra till utvecklingen av Sveriges integritetsskyddspolitik.

Förslaget att ge IMY i uppdrag att kontinuerligt lämna en redovisning till regeringen av utvecklingen på it-området när det gäller ny integritet och teknik lämnades ursprungligen av Integritetskommittén år 2016.[6] Utöver att regeringen tar del av rapporten, menade kommittén att det bör införas en ordning där regeringen överlämnar rapporten till riksdagen i form av en skrivelse som även innehåller regeringens egna kommentarer till rapporten.

Kommittén anförde att såväl regeringen som riksdagen har behov av kunskap för att kunna följa den snabba teknikutveckling. Kunskap behövs till exempel om vilka trender som kommer att vara av betydelse i framtiden och om hur stort det sammanlagda trycket blir på den enskilda individens privata sfär. Sådan kunskap behövs för att på olika sätt kunna påverka utvecklingen i önskvärd riktning. Kommittén menade även att kunskapen är värdefull exempelvis när det gäller att bedöma dels behov av ny lagstiftning, dels effekterna av befintlig lagstiftning och andra åtgärder som innebär att enskilda registreras eller kartläggs.[7]

6. SOU 2016:41 *Hur står det till med den personliga integriteten?*, sid. 647 ff.

7. Dataskyddsmyndigheterna har också enligt dataskyddsförordningen i uppdrag att följa utveckling som påverkar skyddet av personuppgifter och att ge råd åt bland annat riksdag och regering om lagstiftningsåtgärder och andra administrativa åtgärder rörande skyddet för fysiska personers rättigheter och friheter när det gäller behandling av personuppgifter. Se förordningen artikel 57 där tillsynsmyndigheternas uppdrag regleras.

2.1.1 Målgrupp, syfte och innehåll

Rapporten riktar sig i första hand till regering, riksdag och andra policyskapande beslutsfattare som har ett behov av att få ökad kunskap om och förståelse för teknikutveckling och integritetsskyddsfrågor. Även dataskyddsombud och andra som arbetar mer praktiskt med dataskydd, informations- eller cybersäkerhet kan sannolikt ha behållning av olika delar i rapporten.

Syftet med rapporten är att

- öka den allmänna kunskapen om teknikutvecklingen och vilka teknikutvecklingsområden som har störst betydelse för den personliga integriteten
- ge en översiktlig bild av hur bra Sveriges integritetsskydd är idag
- belysa vissa åtgärder som genomförts som har central betydelse för integritetsskyddet
- fungera som underlag för prioriteringar av ytterligare åtgärder och bidra till utvecklingen av Sveriges integritetsskyddspolitik.

Arbetet med att ta fram rapporten har dessutom gett erfarenheter och kunskaper som kan komma till nytta i IMY:s egen verksamhet framöver.

Rapportens kärna utgörs av en beskrivning av utvecklingen när det gäller digitalisering och ny teknik som återfinns i kapitel 5. Teknikavsnittet föregås av inledande beskrivningar av de nyttor som finns med en ökad användning av data som strategisk resurs, hur personlig integritet kan förstås och varför det är viktigt (kapitel 2), en beskrivning av den politik som bedrivs på området inom EU och i Sverige (kapitel 3) samt en sammanfattning av vilka krav regelverket ställer på skyddet av personuppgifter (kapitel 4).

Efter teknikavsnittet följer beskrivningar av hur bra integritetsskyddet kan sägas vara idag, utifrån ett antal iakttagelser från IMY:s verksamhet (kapitel 6), och även en kort sammanställning av forskningsinitiativ som bedrivs inom området (kapitel 7) i syfte att bland annat adressera hur tekniken kan fortsätta att utvecklas och samtidigt säkerställa den personliga integriteten.

Rapportens viktigaste slutsatser och rekommendationer återfinns tillsammans med sammanfattningen i början av rapporten (kapitel 1).

2.1.2 Metod och avgränsningar

Arbetet med rapporten inleddes med att ett tiotal intervjuer genomfördes med experter inom integritet, ny teknik, dataskydd och angränsande områden. Under intervjuerna ställdes frågor om bland annat vad de intervjuade ansåg varit den mest aktuella och betydelsefulla utvecklingen som påverkat den personliga integriteten under de senaste tre åren och om det finns eventuella riskområden som de ansåg bör uppmärksammas särskilt. Slutsatserna från intervjuerna har, tillsammans med IMY:s egna bedömningar och erfarenheter, legat till grund för rapportens övergripande inriktning och urvalet av de områden vi valt att fokusera på. I vissa delar återges också exempel, uttalanden eller slutsatser från experterna.

Materialet i rapporten bygger primärt på omvärldsbevakning där bland annat olika redovisningar av regeringsuppdrag, forskningsprojekt, rapporter från konsultföretag och nyhetsartiklar ingår, slutsatser från rapporter och beslut som IMY eller andra dataskyddsmyndigheter tidigare publicerat samt erfarenhet hos IMY:s specialister. En viktig informationskälla har också varit externa möten och samverkan som myndigheten löpande har med andra myndigheter och organisationer. Även i utformningen av rapportens slutsatser och rekommendationer har dialog förts med vissa nära samverkansparter till IMY.

Rapporten är inte avsedd att användas som vägledning för praktiskt arbete med dataskydd och informationssäkerhet. Sådan vägledning ges i första hand på dataskyddsområdet i de EU-gemensamma vägledningar som arbetas fram inom ramen för Europeiska dataskyddsstyrelsen, EDPB.[8]

Rapporten gör inte anspråk på att vara heltäckande. Stora datamängder finns i alla delar av samhället och risker för den personliga integriteten kan variera beroende på sektorspecifika förutsättningar. Området är därför mycket omfattande. Teknikutvecklingen går också mycket fort, vilket snabbt kan göra iakttagelser om ny teknik inaktuella. Mer djupgående tekniska beskrivningar saknas genomgående. Rapporten gör slutligen inte heller anspråk på att utgöra ett fullständigt kunskapsunderlag. Utgångspunkten har i stället tagits i IMY:s uppdrag och utifrån det adresseras frågor som aktualiseras i verksamheten och omvärlden.

2.2 Ökad användning av data – varför är det viktigt?

Rapporten tar avstamp i konstaterandet att det finns en stark ambition i Sverige och övriga EU att öka förmågan att bli ännu bättre på att analysera och skapa värde av stora mängder data.

Datadriven utveckling innebär helt nya förutsättningar för att skapa ett bättre samhälle, nu och för kommande generationer. Samhällsutmaningar som miljö- och klimatarbete, en utvecklad och mer effektiv välfärd och medicinsk forskning är viktiga exempel där den nya tekniken kan göra omvälvande nytta.

Tillgången till stora mängder data är i mångt och mycket bränslet i den pågående digitaliseringen. I Sveriges digitaliseringsstrategi konstaterar regeringen att möjligheten att analysera stora datamängder öppnar för ny kunskap som inte varit möjlig att erhålla på annat sätt.

Inom en rad områden ger utvecklingen hopp om att bättre kunna möta samtidens stora samhällsutmaningar, inte minst i miljö- och klimatfrågor. Genom nya sätt att resa, bo, konsumera, kommunicera och leva kan vi bli bättre på att tillvarata och bevara jordens resurser på ett hållbart sätt. Digitalt drivna innovationer kring vägar, transporter och varuflöden kan till bidra till att minska klimat- och miljöpåverkan. Samhällsplaneringen blir mer ändamålsenlig när dimensioneringen av samhällskritiska funktioner som vatten- och energiförsörjning och annan infrastruktur kan bygga på analys av stora mängder data. Även livsmedelsproduktion kan optimeras.

Datadriven utveckling har stor potential i utvecklingen av den offentliga välfärden. Nya digitala metoder och arbetssätt kan bidra till att höja kvalitet och effektivitet inom till exempel hälso- och sjukvården och skolan – men också skapa förutsättningar för en mer jämlik och likvärdig offentlig service i hela landet. Att analysera stora mängder data är sedan länge också en central metod för att skapa ett tryggare och säkrare samhälle, till exempel att analysera mobildata i brottsutredningar eller att kartlägga finansiella transaktioner för att förebygga och upptäcka bedrägerier och penningtvätt.

8. https://edpb.europa.eu/.

Ytterligare ett område där användning av persondata skapar stora värden är den mediciniska forskningen. Med utgångspunkt i analyser av stora mängder patientdata kan nya metoder utvecklas för att upptäcka allvarliga sjukdomar, förbättra behandlingar och minska biverkningar.

För såväl privat som offentlig verksamhet medför tillgången till och användningen av data möjligheter att bättre förstå användares beteenden och behov och därmed kunna erbjuda mer användarcentrerade produkter och tjänster. Innovation och utveckling bidrar därmed till att skapa värde för såväl medborgare och kunder som företag, myndigheter och andra organisationer.

Några exempel på konkreta användningsområden där analyserad data kan skapa stora värden är

- för att utveckla och effektivisera eller skapa helt nya former av befintliga produkter och tjänster
- för att mer precist kunna följa upp och kontrollera utrustning, flöden, anställda och andra delar i en verksamhet
- för att bättre förstå och kunna möta medborgares och kunders behov och beteenden
- för att kunna förutse, och därmed påverka, människors beteenden
- för att ta fram prognoser och scenarier och förutse utvecklingen inom olika områden
- inom forskningen.

Sammanfattningsvis är användningen av data en viktig förutsättning för att forskning och utveckling ska kunna bidra till ett bättre samhälle, nu och för kommande generationer.

2.3 Vad innebär personlig integritet och varför är det viktigt?

För att den digitala utvecklingen ska vara hållbar är det avgörande att datadriven innovation kombineras med kraftfulla insatser för att värna den personliga integriteten. Kärnan i personlig integritet handlar om den enskildes rätt till ett privatliv och rätten till självbestämmande. Ett *privatliv* innebär att ha möjlighet att ha privata tankar och förtrolig kommunikation utan att bli kartlagd, spårad eller övervakad. *Självbestämmande* handlar om att själv kunna kontrollera uppgifter som rör en själv, vem som använder uppgifterna och varför.

Rätten till skydd för den personliga integriteten och skyddet för privatlivet är *grundläggande rättigheter* som skyddas av internationella konventioner, EU-rätten och svensk grundlag. Det är också i hög grad en *demokratifråga* eftersom det är svårt att utöva andra grundläggande rättigheter som åsikts-, yttrande- och organisationsfrihet om inte integritetsskyddet finns på plats. Därtill är ett gott integritetsskydd en *hållbarhetsfråga*, så att de system och processer vi nu skapar för att utvinna och använda data inte omöjliggör för kommande generationer att utnyttja sina rättigheter.

När skyddet av personuppgifter fallerar kan konsekvenserna för den enskilde bli till exempel olika former av bedrägerier och it-brott. Det gör att integritetsskydd har stor betydelse för *individers säkerhet*.

Stora mängder uppgifter om andra länders medborgare kan vara ett reellt geopolitiskt maktmedel. Ett gott integritetsskydd får därmed också konsekvenser för *samhällets säkerhet*. Det finns viktiga överlappningar och beröringspunkter mellan arbetet med informations- och cybersäkerhet, dataskydd och säkerhetsskydd.

Hur begreppet personlig integritet ska definieras är inte självklart. Det finns ingen allmänt vedertagen definition, vilket konstaterats bland annat i lagstiftningssammanhang. I de utredningar som gjorts om personlig integritet under de senaste 50 åren återfinns dock en tydlig röd tråd som handlar om individens rätt till en privat sfär och rätten till självbestämmande.

I vidare mening omfattar begreppet personlig integritet även rätten till skydd mot godtyckliga ingripanden som rör till exempel familj, hem eller korrespondens. I denna rapport ligger dock fokus på personlig integritet som rör skyddet av personuppgifter.

Redan 1966 års Integritetsskyddskommitté menade att integritetsbegreppet var liktydigt med den enskildes anspråk på att information om hans eller hennes privata angelägenheter inte ska vara tillgänglig för eller få användas av utomstående utan hans eller hennes vilja.[9] Drygt 20 år senare konstaterade Data- och offentlighetskommittén att, även om det fanns ett antal olika definitioner av personlig integritet, så innehöll de så gott som alltid moment av dels den enskildes rätt till en fredad sektor, dels rätten till självbestämmande. Gemensamma nämnare i de olika definitionerna var ofta den enskilde individens rätt att själv bestämma vilka uppgifter om sig själv och sina personliga förhållanden som individen ska lämna ifrån sig samt hur dessa uppgifter ska få användas och spridas.[10]

I och med dataskyddsdirektivet och ikraftträdande av personuppgiftslagen, PUL, 1998, kom begreppet personlig integritet i Personuppgiftslagsutredningens översyn av personuppgiftslagen från 2004 att riktas mot automatiserad behandling av personuppgifter.[11]

Integritetsskyddskommittén från 2008 förde ett likartat resonemang som tidigare utredningar och konstaterade att det inte var möjligt, eller i vart fall inte meningsfullt, att formulera en definition av personlig integritet som pekar ut alla situationer i vilka individen har en rätt att få sin integritet respekterad och skyddad. Kommittén beskrev dock ett antal moment i den personliga integriteten som är av grundläggande betydelse när rättighetsinskränkande åtgärder övervägs. För det första rätten till skydd av individens kroppsliga integritet, privata tankar och förtrolig kommunikation med andra samt den enskildes möjligheter att själv avgöra om andra ska få ta del av känsliga uppgifter som rör till exempel hälsa eller sexualliv. För det andra måste det alltid finnas ett skydd för rätten att ”stänga om sig”, det vill säga utgångspunkten måste vara att den enskilde ska vara fri att kunna avskärma sig från omgivningen.[12]

Även Integritetskommittén från 2016 fann att det inte var meningsfullt att försöka finna en precis definition av begreppet personlig integritet, bland annat eftersom rätten till en privat sfär inte är absolut utan relaterad till en rad olika omständigheter, som dessutom kan variera över tid. Kommittén fokuserade i första hand på digital insamling, användning och spridning av uppgifter – inklusive bilder – om enskilda och deras personliga förhållanden. Utgångspunkt togs i den enskildes rätt till privata tankar och förtrolig kommunikation med andra, samt den enskildes möjligheter att själv avgöra vem som i olika sammanhang ska få ta del av uppgifter som rör denne. I den rätten ligger även ett skydd mot registrering, spridning eller annan behandling av felaktiga, kränkande eller påhittade uppgifter.

Genom dataskyddsförordningens införande har enskildas rättigheter stärkts. Förordningen syftar till att stärka enskilda individers integritet genom bland annat skydd mot att uppgifter behandlas utan lagligt stöd och rätt till information om, kontroll över och insyn i hur deras personuppgifter behandlas.

Även om någon fast definition inte slås fast här och även om rättigheten inte är absolut, bör personlig integritet i det digitala samhället sammanfattningsvis kunna förstås som den enskildes rätt till

- **Privatliv.** Rätten att få vara ifred, ha privata tankar och kunna kommunicera förtroligt med andra utan att bli kartlagd, spårad eller övervakad.
- **Självbestämmande.** Att själv kunna kontrollera personuppgifter som rör en själv, vem som använder uppgifterna och för vilka syften. Detta är särskilt angeläget när det handlar om vem som ska få ta del av känsliga uppgifter som rör till exempel hälsa eller sexualliv.

I dataskyddsförordningen och andra regelverk på området används genomgående begreppet dataskydd. Integritetsskydd kan i denna kontext förstås som åtgärder (i ett bredare perspektiv) som vidtas för att skydda den personliga integriteten, medan dataskydd i någon mån är ett snävare begrepp där fokus ligger på att uppfylla lagstiftningens krav och intentioner i fråga om behandling av personuppgifter.

9. Data och offentlighetskommitténs delbetänkande *Integritetsskyddet i informationssamhället 3, Grundlagsfrågor*, Ds Ju 1987:8.

10. Data och offentlighetskommitténs delbetänkande *Integritetsskyddet i informationssamhället 3, Grundlagsfrågor*, Ds Ju 1987:8.

11. Personuppgiftslagen (1998:204); Personuppgiftslagsutredningens betänkande *Översyn av personuppgiftslagen*, SOU 2004:6.

12. Integritetsskyddskommitténs slutbetänkande *Skyddet för den personliga integriteten, Bedömningar och förslag*, SOU 2008:3.

2.3.1 Personlig integritet – en mänsklig rättighet

Personlig integritet är en grundläggande mänsklig rättighet som skyddas av internationella konventioner, EU-rätten och svensk grundlag.

Rätten till privatliv uttrycks i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR). Grundläggande är rätten till respekt för privat- och familjeliv, hem och korrespondens.[13] Konventionen har införts som lag i Sverige. Även i EU:s stadga om grundläggande rättigheter uttrycks rätten till respekt för privat- och familjeliv. Här finns också en särskild bestämmelse om rätt till skydd för personuppgifter.[14] Stadgan är rättsligt bindande för EU:s medlemsstater.

I regeringsformen finns regler om rätt till skydd för den personliga integriteten.[15] Bland annat ges skydd mot hemlig avlyssning och mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Utgångspunkten i dataskyddsförordningen är också rättighetsperspektivet – att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.[16]

Tas utgångspunkt i ett filosofiskt perspektiv snarare än ett rättsligt kan man på ett övergripande plan säga att det finns två olika huvudtyper av teoretiska skolor om personlig integritet; de som betonar den personliga integritetens betydelse för individen och de som snarare framhåller den personliga integritetens betydelse för kollektivets utveckling.[17]

I centrum för mer individualistiska teorier står den enskildes makt över sitt eget liv och ett begränsande av myndigheters godtyckliga makt. Rätten till personlig integritet är avgörande för att varje människa ska kunna bestämma vem han eller hon vill vara. En viktig aspekt av detta är den enskildes rätt att kontrollera uppgifter om henne eller honom och utflödet av sådan personlig information.

13. Artikel 8 dataskyddsförordningen.
14. Artikel 7–8 dataskyddsförordningen.
15. 2 kap. 6 § andra stycket regeringsformen.
16. Artikel 1.2 dataskyddsförordningen.
17. En mer utförlig genomgång av olika teorier om personlig integritet finns i Integritetskommitténs delbetänkande från 2016; *Hur är det ställt med den personliga integriteten*, SOU 2016:41, sid. 136–141.

Ur ett individperspektiv har reflekterats över hur vi påverkas av att inte ha tillgång till oövervakade och fria rum, där vi tryggt kan dela frågor, erfarenheter, personliga upplevelser och utvecklas i dialog med våra närmaste. I en publikation redan från slutet av 1960-talet[18] konstaterades att skyddet av den personliga integriteten bland annat är viktigt för att individen ska uppnå en känsla av personligt självbestämmande, ett känslomässigt lugn, att fritt kunna värdera andra människors och sitt eget handlande samt att kunna kommunicera fritt med andra efter eget val.

I diskussioner om personlig integritet hörs ibland uppfattningen ”jag har ingenting att dölja”, vilket skulle legitimera en vid användning av personuppgifter. Poängen med ett starkt integritetsskydd är dock den enskilda individens *rätt att välja själv*. För vissa kan detta innebära att ”inte dölja någonting”, medan andra kan föredra att vara mer återhållsamma med vilken information de delar med sig av och till vem. De grundläggande mänskliga rättigheterna tillförsäkrar alla individer ett grundläggande skydd, som staten bedömt ska utgöra en gemensam skyddsnivå för alla, oavsett var individer i enskilda fall anser att gränsen borde gå. De skyddar på så sätt både individerna och kollektivet.

2.3.2 Personlig integritet – en demokratifråga

Förutom att personlig integritet är en rättighet som fyller en rad behov och syften för enskilda individer finns också ett antal argument och teorier som betonar den personliga integritetens betydelse för kollektivet och samspelet mellan människor.

Rätten till privatliv är en förutsättning för att kunna utöva andra grundläggande rättigheter som åsikts-, yttrande- och organisationsfrihet. Skyddet av den personliga integriteten, som är en del i rätten till privatliv, är därmed i hög grad en demokratifråga. Ett väl utvecklat offentligt samtal och en frisk demokrati förutsätter oövervakade fria och privata rum där vi kan pröva tankar och åsikter innan vi eventuellt väljer att bli mer publika.

Det är en viktig förutsättning för samspelet mellan människor att den enskilde individens rätt respekteras. Det innebär att den enskilde i varje ögonblick har vetskap om vilka personuppgifter som behandlas om honom eller henne och varför samt att den enskilde själv kan avgöra om uppgifterna ska vara publika eller komma andra till del. En uppgift som inte är känslig i ett visst sammanhang kan upplevas som djupt personlig och integritetskänslig i ett annat. Även skälen till att vi vill hålla information för oss själva kan variera. Det kan handla om vardagliga och sociala behov, men också om skydd för till exempel vår åsiktsfrihet, vår fysiska säkerhet eller rättssäkerhet.

18. Alan Westin, *Privacy and Freedom*, 1967.

Även vissa former av ekonomiskt samspel i samhället bygger på att vi, om vi vill, kan begränsa vilken information andra har om oss. Det kan till exempel handla om strategiska överväganden i en förhandlings- eller budgivningssituation.

Ur ett samhällsperspektiv är det angeläget att säkerställa ett grundläggande skydd för alla människor, som drar upp riktlinjerna för vårt samspel och grundläggande demokratiska värderingar. Det är särskilt angeläget att säkerställa skyddet för vissa skyddsvärda grupper, till exempel barn och unga. När barns och ungas vardagsliv i allt högre utsträckning utspelar sig i digitala miljöer är det centralt att deras fri- och rättigheter värnas där, precis som i den fysiska världen. Barn och unga rör sig snabbt och vant mellan olika digitala tjänster, men det är inte alltid synonymt med att de inser risker eller förstår konsekvenser av det, konsekvenser som dessutom kan ligga långt in i framtiden.

2.3.3 Personlig integritet – en hållbarhetsfråga

För att samhället ska kunna utnyttja digitaliseringens möjligheter på ett hållbart sätt är en förutsättning att människor, företag och organisationer känner tillit till digitala tjänster.

Om människor känner oro för att deras personuppgifter hanteras felaktigt finns en risk att de väljer att avstå från att använda en digital tjänst. I en undersökning som IMY genomförde 2019 uppgav hälften av de tillfrågade individerna att de ibland eller ofta avstår från att använda en digital tjänst om de upplever osäkerhet kring hur deras personuppgifter kommer att hanteras.[19] Att behålla medborgarnas tillit till digitala lösningar är därmed avgörande för att realisera nyttan av digitala investeringar.

Ett antal företag och organisationer har också fått erfara vidden av den förtroendeskada en personuppgiftsincident kan orsaka. I en hållbar affärsmodell är därför ett effektivt integritets- och dataskydd avgörande för långsiktig affärsutveckling och hållbar lönsamhet.

Integritetsskydd kan även ses som en hållbarhetsfråga i ett mer globalt perspektiv. Hållbar utveckling definieras ofta som ”en utveckling som tillfredsställer dagens behov utan att äventyra kommande generationers möjligheter att tillfredsställa sina behov”.[20] Om vi idag skapar och gör oss beroende av system och processer där vi utvinner och använder stora datamängder på ett oproportionerligt integritetskränkande sätt som medför omfattande möjligheter till kontroll och övervakning, kan kommande generationer komma att påverkas genom att deras möjligheter till en privat sfär och kontroll över deras data i praktiken är satt ur spel.

Bland forskarvärldens skarpaste kritiker av dagens omfattande handel med data har begreppets ”övervakningsekonomi” använts för att beskriva hur hela logiken i marknadsekonomin är under omstöpning.[21] Tesen kan sammanfattas i att den tidigare kapitalismen var industriell, och drevs framåt primärt med naturresurser. Den gick fram med sådan fart att politiken och lagstiftningen inte hann med, och i stora delar av världen har råvaror utvunnits på ett ohållbart sätt.

I den nya digitala kapitalismen upprepar sig mönstret. De stora möjligheterna att tjäna pengar på data driver företag till ett snabbt och målmedvetet utvecklingstempo där politiken har svårt att hinna med. I handeln med data skördas och analyseras nu vårt beteende i detalj, för att i nästa steg kunna förutse och forma vårt beteende. Uttrycket att *om en tjänst på internet är gratis är det sannolikt du som är produkten* hörs ibland för att beskriva de stora digitala plattformarnas och sociala mediernas affärsmodell. Vissa kritiska röster inom akademin går ännu längre och menar att vi inte är produkten – vi är istället råvaran som nu utvinns lika hårdhänt som naturresurser gjort tidigare. För en hållbar digitalisering, där de långsiktiga utmaningarna inte blir lika alarmerande som dagens miljö- och klimatutmaningar, efterlyses bland annat skyddade sfärer där teknologin begränsas samt åtgärder för att begränsa de stora techföretagens makt.

19. Datainspektionens rapport 2019:2 *Nationell integritetsrapport 2019*.

20. http://www.un-documents.net/our-common-future.pdf.

21. Zuboff, Shoshana, *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, 2019.

2.3.4 Personlig integritet – en fråga om individers säkerhet

När skyddet för digitala personuppgifter fallerar kan konsekvenserna i värsta fall bli att information hamnar hos olika hotaktörer. Konkreta risker för den enskilde individen kan då handla om till exempel olika former av bedrägerier eller andra brott.

När det gäller risken att utsättas för brott avgör många gånger sammanhanget om en viss information är känslig eller inte. För många är det sannolikt djupt olustigt om kriminella aktörer får tillgång till uppgifter om en, även om uppgifterna i andra sammanhang uppfattas som förhållandevis harmlösa, som till exempel uppgifter om ålder eller adressuppgifter. Ett exempel kan tas i det stora antal klagomål som inkommit till IMY om så kallade personsöktjänster. Bland klagomålen finns ett antal medborgare som upplever oro för att det är så enkelt att söka fram uppgift om till exempel äldre personer som bor ensamma i ett visst område och som kan utgöra måltavla för olika brottsupplägg.[22]

När allt fler föremål och delar av samhället kopplas upp mot internet öppnas samtidigt upp även för mer fysiska hot mot individers liv, hälsa och egendom. Det kan handla om lokaliseringsdata och kontroll av var personer befinner sig, som möjliggör inbrott och andra brott mot den personliga sfären. Säkerhetsforskare har också demonstrerat hur bristande säkerhet i uppkopplade enheter öppnar upp för fysiska attacker mot människor, utfört på distans, då de bland annat har kunnat ta kontroll över självkörande bilar, men även hacka sig in i medicinisk utrustning som pacemakers och insulinpumpar.[23]

2.3.4.1 Informationssäkerhet och dataskydd – överlappar men skiljer sig också åt

De senaste åren har informationssäkerhet fått allt större fokus i Sverige och kraven har skärpts på verksamheter att vidta åtgärder för att fortlöpande säkerställa att

- informationen alltid finns när vi behöver den (tillgänglighet)
- går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet) samt
- endast behöriga personer får ta del av den (konfidentialitet).

Informationssäkerhet används ofta som ett övergripande begrepp och innefattar skydd av *all* information och i både fysisk som digital form.[24] Dataskydd fokuserar på just personuppgifter och dataskyddsförordningen innehåller särskilda bestämmelser om säkerhetsåtgärder för skyddet av personuppgifter som i stora delar avser åtgärder med bäring på informationssäkerhet. Verksamheter är skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.[25]

Samtidigt som överlappningarna är stora mellan dataskydd och generellt informationssäkerhetsarbete finns en grundläggande skillnad, som handlar om ur vilket perspektiv riskbedömningar sker. Utgångspunkten i dataskyddsförordningen är risker för kränkningar av enskilda individers fri- och rättigheter. Mer konkret kan det resultera i att individer utsätts för olika typer av bedrägerier, finansiell förlust, id-kapning eller diskriminering.

I ett systematiskt informationssäkerhetsarbete bedöms risker ur ett bredare perspektiv. Det handlar om att analysera samtliga tänkbara hot och bedöma hur sannolika de är och vad konsekvenserna blir. Det kan, även här, handla om risker för enskilda medborgare, men här tillkommer också risker för verksamheten.

2.3.5 Personlig integritet – en del av samhällets säkerhet

Som beskrivits ovan är personuppgifter en typ av information som regleras särskilt i dataskyddsreglerna. Andra uppgifter omfattas av informationssäkerhetsregelverket då information i olika verksamheter ska klassas ur ett informationssäkerhetsperspektiv. Mer känsliga uppgifter kräver en högre skyddsnivå och säkrare hantering. Det finns även särskild reglering kring information som är sekretessbelagd med hänsyn till Sveriges säkerhet genom säkerhetsskyddsregleringen.[26]

Säkerhetsskydd handlar om att skydda information och verksamheter som är av betydelse för Sveriges säkerhet mot spioneri, sabotage, terroristbrott och vissa andra hot.

22. Datainspektionen rapport 2020:1 *Klagomål mot personsöktjänster med frivilligt utgivningsbevis maj 2018–oktober 2019*.
23. The Economist; *A connected world will be a playground for hackers*, 2019 https://www.economist.com/technology-quarterly/2019/09/12/a-connected-world-will-be-a-playground-for-hackers.
24. Myndigheten för samhällsskydd och beredskap, MSB, har i uppdrag att samordna och stödja samhällets arbete med informationssäkerhet.
25. Artikel 5.1 f, 24 och 32 dataskyddsförordningen.
26. Säkerhetspolisen är tillsynsmyndighet på området.

Det förändrade säkerhetspolitiska läget i Sveriges omvärld i kombination med teknikutvecklingen har medfört ett ökat hot som riskerar att få allvarliga konsekvenser för samhällets funktionalitet. Säkerhetspolisen, som är tillsynsmyndighet för de flesta myndigheter när det gäller säkerhetsskyddslagen, har vid upprepade tillfällen beskrivit hur främmande makt i takt med teknikutvecklingen använder allt fler metoder för att inhämta information. Inhämtningen av känsliga uppgifter sker hela tiden och riktas mot såväl våra grundläggande individuella rättigheter, vårt ekonomiska välstånd, vårt politiska oberoende som vår territoriella suveränitet. Syftet är bland annat att kunna destabilisera Sverige som nation – om eller när det behövs. Detta innebär ett nytt, fördjupat säkerhetshot. Säkerhetspolisen understryker att teknikutvecklingen inom till exempel 5G och utvecklingen av Internet of Things, IoT, kommer att påverka Sveriges säkerhet för lång tid framåt. Den snabba digitaliseringen i kombination med fortsatt stora brister i it-säkerheten bedöms av Säkerhetspolisen innebära att riskerna för störningar i samhällsviktiga verksamheter ökar.[27]

Sverige fick 2019 en ny säkerhetsskyddslag i syfte att öka Sveriges gemensamma förmåga att stå emot angrepp.[28] Den som bedriver säkerhetskänslig verksamhet ska genomföra en säkerhetsskyddsanalys och dokumentera den. Viktiga frågor i säkerhetsskyddsanalysen är om verksamheten hanterar säkerhetsskyddsklassificerade uppgifter, vilka antagonistiska hot som finns mot verksamheten och vilka skyddsåtgärder som är nödvändiga. Säkerhetsskyddsåtgärder ska vidtas inom områdena informationssäkerhet, fysisk säkerhet samt personsäkerhet.

Såväl inom Sverige och inom EU används också allt oftare begreppet cybersäkerhet. Antagonistiska hot som riktar sig mot digitala system och digital information benämns cyberhot, och arbetet med skyddsåtgärder som cybersäkerhet. I EU:s cybersäkerhetsakt definieras cybersäkerhet som ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot”. Definitionen beaktar med andra ord den antagonistiska faktorn.[29]

Sammanfattningsvis finns tydliga överlappningar mellan dataskydd, informations- och cybersäkerhet samt säkerhetsskydd – men också skillnader i vilken utgångspunkt som tas för arbetet. Arbetet med dataskydd fokuserar på personuppgifter och risker för enskilda, medan informationssäkerhet innefattar samtliga typer av information, hot och risker. Arbetet med säkerhetsskydd tar istället sikte på det som ur ett samhällsperspektiv är allra mest skyddsvärt, till exempel verksamheter inom totalförsvaret, rättsväsendet, energi- eller vattenförsörjningen, telekommunikationer eller transportsektorn. I cybersäkerhetsbegreppet ligger fokus på antagonistiska hot. Gemensamt för alla områdena är skyddet för information som genom den snabba digitaliseringen och teknikutvecklingen blir allt mer angeläget.

Förenklat kan förhållandet mellan informationssäkerhet, dataskydd, cybersäkerhet och säkerhetsskydd beskrivas som i tabellen nedan – där informationssäkerhet är den övergripande benämningen för skydd av all information.

Tabell 1. Förhållandet mellan informationssäkerhet, dataskydd, cybersäkerhet och säkerhetsskydd.

	Informationssäkerhet	Dataskydd	Cybersäkerhet	Säkerhetsskydd
Typ av information som skyddas	All information	Personuppgifter (alla uppgifter som avser en identifierad eller identifierbar individ)	All digital information	Information som är sekretessbelagd med hänsyn till Sveriges säkerhet
Utgångspunkt i risk- och konsekvens-bedömningar	Alla typer av risker som påverkar den aktuella verksamheten	Risker för enskilda individers fri- och rättigheter	Risker kopplade till cyberangrepp eller cybersårbarheter	Hot, sårbarheter och skyddsåtgärder av betydelse för Sveriges säkerhet
Typ av hot som beaktas	Alla hot	Alla hot	Antagonistiska cyberhot	Antagonistiska hot, primärt spioneri, sabotage och terrorism

27. Säkerhetspolisens årsbok 2019.

28. Säkerhetsskyddslag (2018:585), säkerhetsskyddsförordning (2018:658).

29. SOU 2020:58 *EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering.*

Det är centralt att inte se arbetet med dataskydd, informations- och cybersäkerhet och – i förekommande fall – säkerhetsskydd som isolerade företeelser, utan som länkar i en större kedja. De olika perspektiven kräver i stor utsträckning samma typ av kontinuerligt och systematiskt arbete, där risker (ur alla olika perspektiv) analyseras löpande och ligger till grund för att utforma, genomföra och följa upp åtgärder. Verksamheter som strävar efter att integrera de olika perspektiven i ett och samma ledningssystem har sannolikt större förutsättningar att nå kvalitet och ett effektivt skydd för uppgifterna och också för verksamheten.

En av de viktigaste förändringarna i den nya säkerhetsskyddslagen är att den omfattar fler verksamheter än tidigare lagstiftning på området och att det i lagstiftningen förtydligats att det gäller både privata och offentliga verksamheter.

Att arbetet med olika former av säkerhet gällande information är sammanlänkande innebär att de också ger stöd åt varandra. Det innebär att dataskyddsförordningen, som gäller alla verksamheter som hanterar personuppgifter, skapar en grund för en stark informationssäkerhet i Sverige. Det påverkar i sin tur även cybersäkerheten och Sveriges förmåga att stå emot riktade angrepp. Samtidigt är ett skydd mot angrepp på samhället en viktig förutsättning för att det offentliga ska kunna skydda den enskildes rätt till privatliv.

Ur ett riskperspektiv är det i vissa fall svårt att dra skarpa gränser mellan vad som är en risk för enskilda individer och vad som utgör risker för Sveriges säkerhet. Ett exempel kan tas i den omfattande personuppgiftsincident som under 2018 uppdagades hos hotellkedjan Marriott. Under flera års tid hade en antagonistisk hotaktör haft olovlig åtkomst till namn, kontaktuppgifter, födelsedatum, passnummer och andra personuppgifter i hotellets databas. Totalt drabbade intrånget, som enligt internationell media kunde spåras till kinesiska aktörer, cirka 500 miljoner medborgare.[30] Överträdelsen resulterade i en av de hittills största sanktionsavgifterna från någon dataskyddsmyndighet i Europa när brittiska ICO beslutade om en sanktionsavgift på 20 miljoner Euro. Ett annat välkänt exempel är företaget Cambridge Analytica, där data om över 50 miljoner användare som utvunnits i ett personlighetstest på Facebook, skapat psykologiska profiler som använts i den amerikanska presidentvalskampanjen.

Andra exempel från de senaste åren på hur dataskyddsfrågor och säkerhetsskydd överlappar kan tas i avslöjandet om hur data från en träningsapp kan användas för att lokalisera såväl hemliga militärbaser som enskilda soldater. Den positioneringsdata som samlats in när användare laddat upp sina löpturer i träningsappen Strava visade sig vara så detaljerad att information om både militärt känsliga platser och persondata riskerade att röjas. Ytterligare ett exempel rör it-attacken mot det finska vårdbolaget Vastaamo, där tusentals patientjournaler läckt ut och patienter vars uppgifter läckt har utpressats för att stoppa spridningen av de privata uppgifterna på nätet. Om en sådan attack skulle omfatta även personer i säkerhetsklassade befattningar skulle utpressning kunna användas av främmande makt för att till exempel förmå individer att delta i spionage.

Händelserna ovan omfattas primärt av lagstiftningen på dataskyddsområdet, men får konsekvenser även ur ett säkerhetsskyddsperspektiv. Stora mängder uppgifter om andra länders medborgare är ett reellt geopolitiskt maktmedel som kan underlätta eventuella framtida angrepp. World Economic Forum, WEF, listade i sin riskanalys år 2019 cyberhotet som en av de allra allvarligaste globala riskerna. WEF underströk också att morgondagens geopolitik i stor utsträckning kommer att avgöras av hur olika stater väljer att använda den data de sitter på om sina egna och andra staters medborgare.[31]

30. New York Times; *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

31. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

3. Integritetsskyddspolitiken i EU och Sverige idag

Både på EU-nivå och i svensk politik finns idag en ambitiös digitaliseringspolitik med ett uttalat mål om att vara bäst i världen på att ta tillvara digitaliseringens möjligheter. I det här kapitlet beskriver vi ett antal viktiga digitaliseringspolitiska initiativ som tagits de senaste åren och som påverkar den personliga integriteten.

Vi konstaterar att det saknas en uttalad politik och en allmänt vedertagen definition av det politikområde som rör den personliga integriteten, men väljer att beskriva politikområdet under rubriken ”integritetsskyddspolitik” och beskriver ett antal åtgärder som vidtagits de senaste åren. Den viktigaste förändringen handlar om att dataskyddsreformen genomförts.



3.1 EU:s digitaliseringspolitik

Digitalisering är ett av EU:s högst prioriterade områden. I februari 2020 presenterade EU-kommissionen tre strategiska dokument som anger inriktningen för EU:s digitala framtid: en övergripande digitaliseringsstrategi, en datastrategi och en vitbok om AI.

***EU:s digitaliseringsstrategi* listar ett antal konkreta åtgärder som tillsammans ska skapa värde för medborgare, för företag och för samhället i stort. Föreslagna åtgärder med bäring på integritetsskyddsfrågorna är bland annat ett utvecklat regelverk kring internetplattformars ansvar samt strategier för kvantdatorer och blockkedjeteknik.**

***Datastrategin* innehåller åtgärder för att utveckla ett rättsligt ramverk kring dataanvändning, ökade investeringar för att stärka kapaciteten att använda data, åtgärder för att stärka individers möjlighet att kontrollera den egna datan samt åtgärder för att möjliggöra gemensamma europeiska datautrymmen.**

***Vitboken om AI* anger målsättningen att EU ska bli världsledande på AI-teknik, samtidigt som medborgarnas rättigheter säkras. Offensiva satsningar och kraftigt ökade investeringar ska kombineras med ett intensifierat arbete för att tydliggöra ett etiskt och rättsligt ramverk. Som ett första steg i att utveckla det rättsliga ramverket har ett antal etiska principer för användning av AI utarbetats. Framtida regelverk för AI bör enligt kommissionen ha en riskbaserad utgångspunkt, där både bransch och typ av AI-tillämpning beaktas.**

Kommissionens nuvarande ordförande Ursula von der Leyen har sedan hon tillträdde framhållit klimatomställning och digitalisering som kommissionens två prioriterade kärnområden under de närmaste åren. I februari 2020 presenterade kommissionen ett större paket med inriktning för framtidens digitala Europa.

Planen för att ta EU in i framtiden innehåller tre strategiska dokument; en övergripande digitaliseringsstrategi[32], en datastrategi[33] och en vitbok om AI[34]. Dessa innehåller förslag på aktiviteter och åtgärder som kommer genomsyra och prägla initiativ från kommissionen under kommande år och sannolikt också kommer att ställa krav på anpassningar i medlemsstaternas lagstiftning eller på en höjd ambitionsnivå inom respektive område.

3.1.1 Att forma EU:s digitala framtid - EU:s digitaliseringsstrategi

Kommissionens övergripande digitaliseringsstrategi bär rubriken *Att forma EU:s digitala framtid* och presenterar insatser inom tre grundpelare som kommissionen kommer att fokusera på under de kommande fem åren. Det handlar om teknik som skapar genuint värde för medborgare och samhälle, åtgärder för en rättvis och konkurrenskraftig ekonomi och åtgärder för ett öppet och demokratiskt samhälle.[35]

Digital suveränitet är ett centralt begrepp i digitaliseringsstrategin, inte minst i bemärkelsen att minska Europas beroende av amerikanska och kinesiska tech-företag. Kommissionen understryker att EU behöver säkerställa motståndskraften i datainfrastruktur, nätverk och kommunikation. Det kräver enligt kommissionen att Europa skapar rätt förutsättningar för att utveckla och sprida sina egna nyckelförmågor, och därmed minska beroendet av andra delar av världen för de viktigaste teknikområdena. Kommissionen pekar här på följande centrala områden.

Teknik som skapar värde för människor – Fokus ligger på utveckling, etablering och användning av teknik som gör en verklig skillnad i människors dagliga liv och bidrar till en stark och konkurrenskraftig ekonomi som behärskar och formar teknik på ett sätt som respekterar europeiska värden. Centrala åtgärder är bland annat en vitbok om AI (se nedan), en reviderad förordning om superdatorer, en uppdaterad cybersäkerhetsstrategi, europeiska strategier för kvantdatorer och blockkedjeteknik, en översyn av nätverks- och informationssystemsdirektivet (NIS) samt en uppdaterad handlingsplan för 5G och 6G. I paketet finns också en handlingsplan för digital utbildning och en förstärkt kompetensagenda för digitala färdigheter i hela samhället.

32. COM (2020) 67 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om *Att forma EU:s digitala framtid*.

33. COM (2020) 66 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om *En EU-strategi för data*.

34. COM (2020) 65 *Vitbok om artificiell intelligens - en EU-strategi för spetskompetens och förtroende.*

35. Regeringskansliet faktapromemoria 2019/2020 FPM 23; *Digital strategi, AI-vitbok och datastrategi*

En rättvis och konkurrenskraftig ekonomi – Företag i alla storlekar och i alla sektorer ska kunna konkurrera på lika villkor och utveckla, marknadsföra och använda digital teknik i en omfattning som förbättrar deras produktivitet och globala konkurrenskraft och där konsumenterna kan vara säkra på att deras rättigheter respekteras. Centrala åtgärder utgörs bland annat av den europeiska datastrategin – samt ett meddelande om ett rättsligt ramverk för styrning av data samt en eventuell rättsakt om data. Paketet innehåller aktiviteter inom konsument- och konkurrensområdena, bland annat en utredning om konkurrensfrämjande förhandsregler för stora plattformar, som en del av lagpaketet *Digital Services Act*.

Ett öppet, demokratiskt och hållbart samhälle – Fokus ligger på en pålitlig miljö för medborgarna som ska kunna dra nytta av data de tillhandahåller både online och offline, en europeisk metod för digital transformation som stärker demokratiska värderingar, respekterar grundläggande rättigheter och bidrar till en hållbar, klimatneutral och resurseffektiv ekonomi. Centrala åtgärder är bland annat nya och reviderade regler för internetplattformars ansvar, vilket inkluderar en översyn av e-handelsdirektivet, inom ramen för lagpaketet *Digital Services Act* och en översyn av förordningen om elektronisk identifiering med mera. Paketet omfattar också främjande av system för utbyte av medicinska journaler i hela EU.

Sammanfattningsvis kan konstateras att kommissionen har höga ambitioner på digitaliseringsområdet och att ett antal konkreta aktiviteter planeras under kommande år. Aktiviteter med direkt eller indirekt bäring på integritets- och dataskyddsfrågorna samt utvecklingen av ny teknik är bland annat datastrategin, vitboken om AI och förslaget till rättsakt om data som beskrivs nedan. Därtill kommer initiativet om nya och reviderade regler för internetplattformars ansvar och strategier för kvantdatorer och blockchain. Konkreta åtgärder för att höja säkerheten och skydda enskilda individers fri- och rättigheter presenterades också i den uppdaterade cybersäkerhetsstrategi som kommissionen lade fram i december 2020.

Det kan också noteras att ett särskilt fokus för kommissionen är att höja den digitala kompetensen hos medborgare, bland annat genom en handlingsplan för digital utbildning och en förstärkt kompetensagenda för digitala färdigheter.

3.1.2 EU:s strategi för data

Datastrategin beskriver behovet av samlade europeiska insatser för att på ett mer effektivt sätt nyttja data som strategisk resurs. Syftet är att göra EU till den mest attraktiva, säkra, dynamiska och snabbrörliga datadrivna ekonomin i världen, och därmed förbättra beslutsfattande och livskvalitet för samtliga medborgare. Tillgång till samt kontroll över relevanta data, baserat på gemensamma regelverk och standarder, bedöms vara av strategisk betydelse för utvecklingen av digital innovation, särskilt AI, inom EU.

Åtgärderna i datastrategin bygger på fyra områden:

Ett rättsligt ramverk för datatillgång och användning – Kommissionens vision går bland annat ut på att till 2030 skapa gemensamma europeiska datautrymmen som ska kunna stödja utvecklingen inom samhällssektorer som tillverkning, hälsa och mobilitet.

I datastrategin aviserade kommissionen att de under 2020 hade för avsikt att prioritera ett rättsligt ramverk för styrning av gemensamma europeiska datautrymmen. I november 2020 presenterade kommissionen också ett förslag till förordning om dataförvaltning (eng. data governance).[36] Syftet är att ange riktlinjer för utbyte och användning av data, samt prioritera gemensamma övergripande krav och standarder, till exempel om hur forskningsdata kan utbytas i linje med dataskyddsförordningen. Även frågor för att göra det lättare för individer att låta deras data användas för publik nytta i enlighet med dataskyddsförordningen ingår.

Inom ramen för en datarättsakt under 2021 förutser kommissionen också att utveckla rättsliga ramverk som ytterligare ska underlätta delning av data inom näringslivet samt mellan näringslivet och offentlig förvaltning.

Investeringar för att stärka Europas kapacitet för bearbetning och användning data – under perioden 2021–2027 kommer kommissionen att investera 2 miljarder euro för att främja utvecklingen av infrastruktur, verktyg och arkitektur för att dela data och använda AI. Investeringarna kommer bland annat att dedikeras till edge computing, högpresterande datorer och kvantberäkning, cybersäkerhet, lågeffektprocessorer och 6G-nätverk. Projektet ska främja den gradvisa balanseringen mellan centraliserad datainfrastruktur i molnet och distribuerad och smart databehandling genom decentraliserad AI (edge computing).

36. COM(2020) 767 Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om dataförvaltning (*Dataförvaltningsakten*)

Kommissionen betonar också vikten av EU-baserade molntjänstleverantörer. Under 2022 har kommissionen målsättningen att ta fram ett ramverk för de olika reglerna (inklusive självreglering) för molntjänster i form av en ”molnregelbok”. Regelboken kommer att omfatta befintliga molnkoder för uppförande och certifiering av säkerhet, energieffektivitet, servicekvalitet, dataskydd och dataportabilitet.

Stärka individers möjlighet att kontrollera egen data och den digitala kompetensen – genom att förstärka rätten till dataportabilitet enligt dataskyddsförordningen kan individer få mer kontroll över vem som kan få åtkomst till och använda maskingenererade data. Det kan enligt kommissionen handla till exempel om att införa strängare krav på gränssnitt för realtidsdataåtkomst och att göra maskinläsbara format obligatoriskt för data från uppkopplade enheter i hemmet.

Dessutom menar kommissionen att regler för leverantörer av personliga appar och nya dataförmedlare kan övervägas för att garantera att de förmedlar neutral data.

Vidare avser kommissionen att satsa på omfattande utbildningar i ny teknik för att minska behovet av it-specialister, men även basutbildning för att höja medborgarnas digitala kompetens. Särskilt stöd ska också ges till små, medelstora och nystartade företag för att de fullt ut ska kunna nyttja de många möjligheterna som finns i databaserade affärsmodeller.

Gemensamma europeiska datautrymmen – slutligen avser kommissionen att arbeta för utveckling av gemensamma europeiska datautrymmen inom vissa strategiska sektorer. Datautrymmena ska tas fram i enlighet med dataskyddsregler och högsta cybersäkerhetstandard. Syftet är att underlätta innovation och datadriven utveckling. De utpekade sektorerna är industri/tillverkning, miljö- och klimatarbete, mobilitet och transport, hälsodata, finansiella sektorn, energi, jordbruk, offentlig förvaltning och utbildning.

3.1.3 AI ett viktigt fokusområde för EU-kommissionen

Nära förknippad med kommissionens datastrategi är den vitbok om AI som presenterades samtidigt med strategin. Vitboken bygger i stor utsträckning på den AI-strategi som kommissionen lade fram i april 2018.[37] Strategins övergripande målsättning är att EU ska bli världsledande på AI-teknik, samtidigt som medborgarnas rättigheter säkras.

Dessa dubbla huvudspår löper som två tydliga röda trådar såväl genom AI-strategin som genom kommissionens senare dokument på AI-området: offensiva satsningar och kraftigt ökade investeringar ska kombineras med ett intensifierat arbete för att tydliggöra ett etiskt och rättsligt ramverk.

Kopplat till AI-strategin finns en handlingsplan för åren 2019–2025 som understryker att tillämpningen av AI ska främjas och kapaciteten stärkas i alla medlemsstater.

I februari 2020 följde EU-kommissionen upp AI-strategin med en vitbok om AI.[38] Vitboken följer de dubbla huvudspår som kommissionen stakade ut i AI-strategin från 2018: åtgärder för att främja utveckling och användning av AI kombineras med åtgärder för att adressera de risker som finns kopplade till AI- användning.

Vitbokens första del fokuserar på främjande åtgärder för att flytta fram EU:s position att bli världsledande på att utnyttja AI:s möjligheter. Kommissionen konstaterar att investeringarna i forskning och utveckling som avser AI har ökat mycket kraftigt inom EU under de senaste åren. Samtidigt har utvecklingen gått ännu snabbare i andra delar av världen.[39] Kommissionens mål är att AI-investeringarna inom EU ska uppgå till 20 miljarder Euro per år.

Ambitionen är att skapa ett *ekosystem av excellens* som täcker hela värdekedjan från forskning och utveckling till användning av AI. Kommissionen konstaterar att förutsättningarna på många plan är goda; inom EU finns högteknologiska forskningsmiljöer, en stark tech-industri, innovativa startup-företag och god tillgång på offentlig data. Sex åtgärder presenteras i vitboken för att främja AI-utvecklingen. Åtgärderna är:

- att anta en ny version av den samordnande handlingsplanen för AI
- att främja etablerandet av test- och excellensmiljöer
- att stötta universitet och forskningsmiljöer för att attrahera forskare och erbjuda världsledande mastersprogram
- att etablera minst en europeisk digital innovationshubb per medlemsstat med hög specialisering mot AI samt att tillgängliggöra riskkapital för AI-utveckling via den europeiska investeringsfonden
- att inrätta ett offentligt-privat partnerskap för AI, data och robotik samt
- att förbereda ett särskilt program för att stötta offentlig sektor i upphandling av AI-system.

37. https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

38. COM (2020) 65 *Vitbok om artificiell intelligens - en EU-strategi för spetskompetens och förtroende.*

39. Under 2016 investerades 3,2 miljarder Euro i AI inom EU, medan motsvarande siffra för Asien var 6,5 miljarder och 12,1 miljarder för USA.

I vitbokens andra del presenterar kommissionen initiala resonemang för hur ett rättsligt ramverk för AI bör utformas. Det rättsliga ramverket ska bidra till att skapa ett *ekosystem av förtroende* för AI i Europa. De främsta riskerna med AI handlar enligt kommissionen om skyddet för grundläggande rättigheter (inklusive rätten till skydd för privatliv och frånvaro av diskriminering), säkerhet samt frågor om tillförlitlighet. För att säkerställa en proportionerlig reglering förordar kommissionen att ett framtida regelverk för AI bör ha en riskbaserad utgångspunkt. Riskbedömningen bör beakta både vilken bransch AI-tekniken är tänkt att användas i och vilken typ av AI-tillämpning det rör sig om. Sektorer där betydande risker kan förväntas uppstå är till exempel hälso- och sjukvård, transport, energibranschen och delar av offentlig sektor.

För tillämpad AI som bedöms medföra en hög risk anser kommissionen att krav bör ställas på förhandsgranskning, till exempel i form av obligatoriska tester, inspektion och certifiering innan en produkt får släppas på EU:s inre marknad. Utöver detta anger kommissionen att även efterhandskontroller kommer att behövas. För AI-tillämpningar med lägre risk kan ett system med frivillig märkning vara ett alternativ. Som ett första steg behöver en ordentlig analys göras över vilka risker med AI som behöver hanteras och hur befintliga regelverk möter dessa risker. För att möjliggöra en riskbaserad ansats behövs tydliga kriterier för att kunna skilja på AI-tillämpningar med olika risknivåer.

Ett huvudspår i att utveckla ett gemensamt europeiskt etiskt och rättsligt ramverk har varit framtagandet av gemensamma etiska principer för AI. Under de senaste åren har det i enskilda medlemsstater publicerats en stor mängd principer och riktlinjer på temat etik inom AI. Bland upphovsmakarna finns allt från universitet och forskningsinstitut till privata tech-företag eller enskilda länders förvaltningar. Området är dock fortfarande under utveckling och ännu råder ingen internationell samsyn kring vad etisk AI innebär i praktiken. Forskare har i en kartläggning av 84 olika dokument med principer och riktlinjer för etik inom AI konstaterat betydande olikheter i bland annat hur etiska principer som öppenhet, rättvisa, att inte göra skada, ansvarsutkrävande och integritetsskydd ska tolkas, förstås och implementeras.[40]

Mot denna bakgrund har kommissionen sett det som angeläget och brådskande att det inom EU utvecklas gemensamma etiska principer för AI. Risken är annars att skillnader mellan olika medlemsstater försvårar och skapar hinder på EU:s inre marknad.

I juli 2020 publicerade en expertgrupp utsedd av EU-kommissionen ett ramverk med etiska principer och tillhörande bedömningslista för utveckling och tillämpning av AI. Efter att gruppen, som bestod av drygt 50 internationella experter, tagit fram ett första utkast har 350 privata och offentliga aktörer givits möjlighet att testa och komma med synpunkter på de etiska riktlinjerna och den tillhörande checklistan innan den publicerades.[41]

Ramverket innehåller sju etiska principer som beskrivs som centrala för att den fortsatta AI-utvecklingen ska vara säker och pålitlig. De rör 1) mänsklig medverkan och tillsyn, 2) teknisk robusthet och säkerhet under alla faser av ett AI-systems livscykel, 3) dataskydd och kontroll på data; varje medborgare ska ha full kontroll över sin data och att den inte används emot en själv, 4) transparens och öppenhet, 5) mångfald, icke-diskriminering och rättvisa, 6) nyttjande av AI för att lösa samhällsutmaningar, inte minst avseende hållbarhet och miljöfrågor samt 7) ansvarsskyldighet och ansvarsutkrävande.

Kopplat till den etiska principen om dataskydd och kontroll på data innehåller checklistan påminnelser om en rad skyldigheter som följer av dataskyddsförordningen och som kan aktualiseras i utvecklingen och tillämpningen av AI-teknik. I checklistan nämns till exempel följande skyldigheter:

- att utse ett dataskyddsombud och involvera dem tidigt i utvecklingsarbete, upphandlingar och implementering av AI-teknik
- att genomföra en konsekvensbedömning om behandlingen av personuppgifter kan förväntas innebära en hög risk för enskilda individer
- att beakta den grundläggande principen om uppgiftsminimering, i synnerhet när det rör sig om känsliga personuppgifter
- att säkerställa människors grundläggande rättigheter så att det till exempel är möjligt att återkalla ett samtycke, att få felaktiga uppgifter rättade eller att få uppgifter raderade
- att begränsa och kontrollera åtkomsten till data genom till exempel behörighetsstyrning och loggning
- att vidta åtgärder som säkerställer inbyggt dataskydd och dataskydd som standard, till exempel genom kryptering, pseudonymisering, aggregering av data och anonymisering
- att överväga integritetsrisker som kan uppstå löpande under AI-systemets livscykel eller kopplat till data som inte innehåller personuppgifter.

40. Jobin, A., M. Ienca, et al. (2019). *The global landscape of AI ethics guidelines*. Nature Machine Intelligence 1, September 2019, sid. 389-399.

41. The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment.

3.2 EU:s integritetsskyddspolitik – införandet av GDPR och brottsdatadirektivet en historisk reform

Fundamentet i EU:s integritetsskyddspolitik är dataskyddsförordningen, GDPR, som började tillämpas i maj 2018 och brottsdatadirektivet som införlivades i svensk rätt genom brottsdatalagen i augusti 2018.

Dataskyddsförordningen innehåller förstärkta rättigheter för enskilda, som ska kunna utöva insyn och ha kontroll över sina personuppgifter, och utökade skyldigheter för alla verksamheter som hanterar personuppgifter. Förordningen innehåller också helt nya verktyg för korrigerande befogenheter, bland annat kraftfulla sanktionsavgifter.

Dataskyddsförordningen är unik på så sätt att den detaljerat reglerar bland annat dataskyddsmyndigheternas uppdrag och befogenheter och föreskriver att dataskyddsmyndigheten ska vara oberoende.

Genom dataskyddsförordningen inrättades också den Europeiska dataskyddsstyrelsen, EDPB. Genom att EDPB beslutar om riktlinjer men även har mandat att fatta beslut i vissa gränsöverskridande ärenden har styrelsen ett stort mandat – både på policynivå och operativt. I praktiken har en stor del av den nationella suveräniteten när det kommer till tolkning och tillämpning av förordningen samt praxisbildning överlämnats till EDPB.

Kommissionen menade i sin tvåårsutvärdering av dataskyddsförordningen att harmoniseringen mellan länderna ökar, men att det fortfarande behövs en mer enhetlig tillämpning i hela unionen. Kraven på harmonisering har i flera avseenden redan inneburit att IMY behövt anpassa sina arbetssätt.

Ett av de viktigaste stegen i EU:s integritetsskyddspolitik handlar om initiativet att förhandla fram dataskyddsförordningen, GDPR. Förordningen trädde i kraft den 25 maj 2016 men började tillämpas den 25 maj 2018.[42] Lika viktigt var en EU-gemensam reglering av personuppgiftshanteringen på det brottsbekämpande området genomfördes brottsdatadirektivet, som införlivades i svensk rätt genom brottsdatalagen den 1 augusti 2018.[43]

Genomförandet av den nya dataskyddsregleringen är historisk på flera sätt. Dataskyddsförordningen har lagt en grund för all personuppgiftshantering som även genomsyrar regleringen på det brottsbekämpande området och annan dataskyddsreglering. Förordningen innehåller utökade rättigheter för enskilda, som ska kunna utöva insyn och ha kontroll över sina personuppgifter. Dessa rättigheter motsvaras av utökade skyldigheter för alla som hanterar personuppgifter. Förordningen innehåller också helt nya verktyg för korrigerande befogenheter, bland annat kraftfulla sanktionsavgifter.

Utöver att ange det regelverk som gäller på området och återupprepa sedan tidigare gällande krav på ett starkt oberoende för dataskyddsmyndigheterna, kan det som gör reformen historisk sammanfattas i att dataskyddsförordningen

- är en förordning och därmed direkt tillämplig som lag i samtliga medlemsstater
- anger dataskyddsmyndigheternas uppdrag och befogenheter
- inrättar en styrelse, Europeiska dataskyddsstyrelsen (EDPB), som utgör ett eget rättssubjekt, som har att fatta beslut om vägledningar och yttranden samt för tillsynsmyndigheterna bindande beslut i gränsöverskridande ärenden
- innehåller omfattande bestämmelser om krav på harmoniserad tillämpning inom EU
- föreskriver långtgående krav på samverkan mellan dataskyddsmyndigheterna
- anger en tvistlösningsmekanism vid oenighet.

Förordningen har i grunden påverkat företag, myndigheters och andra organisationers dataskyddsarbete liksom tillsynsmyndigheternas verksamhet.

42. Förordningen gäller också för EES-länderna Norge, Island och Lichtenstein.

43. Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (brottsdatadirektivet). I Sverige genomfördes direktivet genom brottsdatalagen (2018:1177) och brottsdataförordningen (2018:1202). Samtidigt trädde nya bestämmelser på kameraområdet i kraft genom kamerabevakningslagen (2018:1200), som ersatte den tidigare kameraövervakningslagen.

3.2.1 Omfattande krav på samverkan och harmonisering inom EU

Det har redan nämnts att dataskyddsförordningen har inneburit stora förändringar för tillsynsmyndigheterna. För att säkerställa ett kraftfullt genomförande regleras, som nämnts, myndigheternas uppdrag och befogenheter i förordningen.[44]

Förordningen ställer krav på en harmoniserad tillämpning inom EU och på långtgående samverkan mellan dataskyddsmyndigheterna. Detta säkerställs genom dataskyddsstyrelsen, EDPB. Styrelsen, som består av respektive lands tillsynsmyndighets chef och Europeiska datatillsynsmannen, EDPS, har till uppgift bland annat att ta fram vägledningar och yttranden. Dessa processas i någon av de närmare 15 arbetsgrupper som förbereder underlag för styrelsen. Beslut om vägledningar och yttranden med mera fattas genom omröstning och de nationella tillsynsmyndigheterna har därefter att anpassa den nationella praxisbildningen utifrån dessa.

En ny ordning, som tar kraven på harmoniserad tillämpning till en ny nivå, är föreskrifter om en enhetlighetsmekanism som ställer krav på samarbete mellan dataskyddsmyndigheterna i ärenden som rör gränsöverskridande behandlingar.[45] Ytterst finns en tvistlösningsmekanism som anger hur frågor ska processas och beslutas om medlemsstaterna inte kan komma överens om hur regelverkets ska tolkas och beslut utformas.[46] Beslutsbefogenheterna för respektive medlemsstat utövas genom röstning och styrelsens beslut i medlemsstatens ärende blir bindande för tillsynsmyndigheterna.

I praktiken innebär inrättandet av EDPB att en stor del av den nationella suveräniteten när det kommer till tillsynsmyndigheternas tolkning och tillämpning av förordningen samt praxisbildning har överlämnats till styrelsen. Utrymmet för de nationella tillsynsmyndigheterna att självständigt ge stöd och vägledning, att göra tolkningar av regelverket i ärendehanteringen och att utmejsla praxis är på så sätt inskränkt. Regelverket ökar kraven på tillsynsmyndigheten att bidra till en harmoniserad tillämpning. Samtidigt ökar behovet av att IMY deltar och tar en aktiv roll i det unionsgemensamma arbetet, i syfte att få så stort genomslag som möjligt för svenska rättstraditioner, att kunna upprätthålla nationell praxisbildning och förvaltningsrättsliga principer. Utan en stark röst riskerar vi att behöva följa en utveckling som vi själva inte varit med och påverkat och som kan strida mot svensk praxis och rättstradition.

44. Artikel 51–59 dataskyddsförordningen.

45. Artikel 56, 60–62 dataskyddsförordningen.

46. Artikel 65 dataskyddsförordningen. Ett (1) ärende har hittills avgjorts efter tvistlösning, https://edpb.europa.com, Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR | European Data Protection Board (europa.eu)

3.2.2 Kommissionen menar att harmoniseringen behöver öka ytterligare

I syfte att säkerställa efterlevnaden av förordningen genomför kommissionen utvärderingar vart fjärde år. Den första genomfördes i anslutning till tvåårsdagen av dataskyddsförordningens införande, våren 2020.[47]

Sammanfattningsvis ansåg kommissionen två år efter införandet av dataskyddsförordningen att förordningen uppfyllt sina mål att stärka skyddet av den enskildes rätt till skydd av personuppgifter och att garantera det fria flödet av personuppgifter inom EU.

Kommissionen konstaterar att harmoniseringen mellan länderna ökar, men att det fortfarande finns viss fragmentisering. Kommissionen pekar på att det framgent behövs en mer enhetlig tillämpning inom hela unionen och att inslagen av nationell lagstiftning behöver minska. För att förordningen ska nå sin fulla potential är det viktigt att skapa ett harmoniserat tillvägagångssätt för gränsöverskridande fall samt en gemensam europeisk datakultur. Kommissionen efterfrågar därför en ännu mer effektiv, harmoniserad hantering vid gränsöverskridande ärenden, samt pekar särskilt på behovet av större samstämmighet avseende förfarandet vid hantering av klagomål. Man vill också se ett ytterligare utökat samarbete mellan dataskyddsmyndigheterna, till exempel genom gemensamma utredningar.

Dataskyddsmyndigheterna bedöms ha en balanserad användning av de stärkta korrigerande befogenheterna. Det konstateras dock att det finns en stor efterfrågan på mer praktisk vägledning och råd som rör tillämpningen av förordningen.

Vissa områden pekas ut där behovet av stöd och vägledning bedöms vara särskilt stort eller där utveckling behövs. Det rör främst

- **Små och medelstora företag** – stöd behövs och praktiska verktyg behöver tas fram, till exempel formulär för personuppgiftsincidenter samt förenklade behandlingsregister.
- **Forskning, hälsa och ny teknik** – stöd behövs i form av riktlinjer för bland annat vetenskaplig forskning, AI och blockkedjeteknik

47. COM (2020) 264 Meddelande från Kommissionen till Europaparlamentet och rådet: *Dataskydd som en pelare för medborgarnas egenmakt och EU:s strategi för den digitala övergången – tillämpning av den allmänna dataskyddsförordningen under två års tid.*

- **Utvecklingen av ny teknik**– dataskyddsförordningen bygger på principer och omfattar ny teknik i takt med att tekniken utvecklas. De framtida utmaningarna består i att klargöra hur de beprövade principerna ska tillämpas på specifik teknik, såsom AI, blockkedjeteknik, IoT eller ansiktsigenkänning. Kommissionen uppmanar dataskyddsmyndigheterna att följa utvecklingen i ett tidigt skede.
- **Medborgarnas kontroll över sin egen data måste bli reell** – enskildas rättigheter behöver stärkas bland annat när det gäller tillgång till och användning av data, till exempel rätten till information och radering av data. Åtgärder behöver vidtas för att underlätta utökad användning av dataportabilitet, och för att ge medborgarna större kontroll över vem som kan få tillgång till och använda maskingenererad data.
- **Särskilda insatser behöver riktas mot barn** – exempelvis behöver frågor om samtycke från barn adresseras och det behövs tydligare riktlinjer gällande användning av barns data.
- **Överföring till tredje land** – det är centralt att verka för att de verktyg som finns för överföring till tredje land används och utvecklas och framåt behövs fokus på att stärka dialogen med verksamheter utanför EU i syfte att stödja likriktningen av dataskyddsreglerna globalt.

3.2.3 Konsekvenser av kraven på harmonisering för Sveriges del

De krav som ställs på harmonisering gäller medlemsstaterna. Olika tolkningar, rättsliga traditioner och nationella regelverk har gjort att tillsynsmyndigheterna går in i samarbetet inom Europeiska dataskyddsstyrelsen utifrån olika förutsättningar. Kraven på harmonisering gäller dock och det är genom dialog, men ytterst genom röstningsförfarande i EDPB, som vägen framåt läggs fast.

Utöver löpande anpassning efter de gemensamma tolkningar som görs och beslut som fattas, har harmoniseringen för Sveriges del bland annat inneburit att vi har fått anpassa vår tolkning av den så kallade one-stop-shopmekanismen. Mekanismen innebär att ett ärende ska utredas där ett företag eller annan verksamhet har sitt huvudsakliga verksamhetsställe,[48] och att ärendet så att säga flyttar med verksamheten om den etablerar sig eller byter huvudsakligt verksamhetsställe under en utrednings gång, vilket för Sveriges del innebar att ett långt framskridet tillsynsärende rörande Google under 2019 fick överlämnas till Irländska dataskyddsmyndigheten för vidare hantering.[49]

Som kommissionen pekar på i sin utvärdering krävs harmonisering i tillsynsmyndigheternas hantering av klagomål. Medlemsstater har haft olika processer för hantering av klagomål. En utredning har pågått under 2019 och 2020 om hur klagomål ska hanteras och beslut fattas inom EDPB i början av 2021 om en gemensam hanteringsordning. Det kommer för Sveriges del innebära att IMY kommer att utreda klagomålen mer ingående och inleda tillsyn i väsentligt många fler fall än tidigare.

I fråga om överföring av personuppgifter till tredje land har EU-domstolen i Schrems II den 16 juli 2020 uttalat att enskildas rättigheter är starka och att det är en förutsättning för att deras rättigheter ska kunna tillgodoses att klagomål i sådana ärenden utreds och att myndigheternas korrigerande befogenheter utnyttjas om utredningen skulle visa att en otillåten överföring av medborgarnas uppgifter sker till USA. Efter domen har ett stort antal klagomål som rör olaglig överföring av personuppgifter till USA kommit in till tillsynsmyndigheterna.[50] Sverige är ansvarig tillsynsmyndighet i sex av dessa ärenden. Samtliga klagomål samordnas genom en särskild arbetsgrupp inom EDPB i syfte att hantera och bedöma dessa på ett enhetligt och harmoniserat sätt.

Kraven på en enhetlig och harmoniserad hantering och bedömning har även i gränsöverskridande ärenden lett till att medlemsstaterna – även Sverige – nu utreder dem och inleder tillsyn i väsentligt högre utsträckning än tidigare.

48. Artikel 56.1 dataskyddsförordningen.

49. IMY drev i EDPB uppfattningen att ett påbörjat tillsynsärende av bland annat effektivitets- och förutsebarhetsskäl bör avslutas av den tillsynsmyndighet som inlett ärendet, även om ett företag under utredningens gång flyttar sitt huvudsakliga verksamhetsställe. Efter omröstning i EDPB landade dock styrelsen i uppfattningen att ärendet ska flyttas om det huvudsakliga verksamhetsstället flyttar.

50. Drygt 100 klagomål som rörde påstådd överföring av personuppgifter till USA lämnades efter Schrems II-domen in av intresseorganisationen NOYB (None of Your Business), som förestås av M. Schrems.

3.3 Exempel på politik inom angränsande lagstiftningsområden

Exempel på EU-lagstiftning som ligger nära integritetsskyddsfrågorna är NIS-direktivet, e-privacydirektivet samt direktivet om öppna data, det så kallade PSI-direktivet.

För att få ett tillämpbart, effektivt och sammanhållet regelverk på integritetsskyddsområdet är det angeläget att övriga lagstiftningsprodukter på EU-nivå harmonierar med förordningen.

Det har, som vi har sett, genomförts ett stort antal initiativ inom EU som rör digitalisering och teknikutveckling, men också integritetsskyddsfrågor. Det finns också ett antal initiativ inom angränsande lagstiftningsområden. Denna utveckling inverkar sällan direkt på utvecklingen inom integritetsskyddsområdet, men när lagstiftningsområden angränsar till varandra och förhandlingsarbetet sker isolerat, finns risk för att regelverken inte harmonierar, medför glapp, eller i alla delar inte går att förena. I sådana fall får myndigheter och verksamheter ett stort ansvar för att tolka och ta ställning i regelkonflikter.

Många gånger ska dataskyddsförordningen tillämpas för personuppgiftsbehandlingen och finns då kompletterande nationell överlappande reglering kan det skapa otydlighet i hur regelverken ska tillämpas. Ett exempel är hur reglerna om samtycke till kakor enligt lagen om elektronisk kommunikation förhåller sig till samtyckesregleringen enligt dataskyddsförordningen. Frågorna rör bland annat hur långt samtycket sträcker sig enligt respektive regelverk och om det ställs samma krav på samtycke enligt lagen om elektronisk kommunikation som enligt dataskyddsförordningen.

Lagstiftning som ligger nära eller i vissa fall specifikt adresserar integritetsskyddsfrågorna är till exempel NIS-direktivet, e-privacydirektivet och förhandlingarna om en ny e-privacyförordning samt direktivet om öppna data, det så kallade PSI-direktivet. Även initiativen inom betaltjänstmarknaden och genomförandet av det andra betaltjänstdirektivet, PSD2, visar hur politiken inom EU verkar för ett fritt flöde av uppgifter, att minska hinder, skapa större förutsättningar för fler aktörer och att det krävs harmoniering mellan regelverken. På nationell nivå ställer det krav på samverkan (i olika konstellationer) mellan myndigheter, bland annat IMY, Myndigheten för samhällsskydd (MSB) och beredskap, Post- och telestyrelsen (PTS), Säkerhetspolisen, Myndigheten för digital förvaltning (DIGG) och Finansinspektionen. Bland annat finns anledning att samordna incidentrapportering som ska ske till olika myndigheter utifrån olika krav, där själva incidenten många gånger är sprungen ur ett och samma händelseförlopp.

Centralt är återigen att påpeka att dataskyddsförordningen är ett centralt regelverk när det gäller personuppgiftsbehandling. Övriga lagstiftningsprodukter på EU-nivå, såväl om det avser förordningar och direktiv som andra lagstiftningsprodukter, behöver ofta harmoniera med förordningen i syfte att skapa ett tillämpbart, effektivt och sammanhållet regelverk på integritetsskyddsområdet. Detsamma gäller också för den kompletterande nationella lagstiftning, som utfärdas som ett led i implementeringen av EU-direktiven i nationell rätt. Här krävs ofta en bred samordning och gemensamberedning mellan olika politikområden i syfte att få en harmoniserad reglering när det gäller personuppgifter inom olika samhällssektorer.

3.4 Sverigesdigitaliseringspolitik

Digitaliseringspolitiken har även på nationell nivå fått en tydlig prioritering de senaste åren, vilket märkts bland annat genom framtagandet av en nationell digitaliseringsstrategi och en nationell inriktning för AI.

***Sveriges digitaliseringsstrategi* anger det övergripande målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Digital trygghet, där personlig integritet ingår, är ett av strategins delmål.**

***Den nationella inriktningen för AI* anger att Sverige ska vara ledande i att ta tillvara möjligheterna som användning av AI kan ge. I den nationella inriktningen konstaterar regeringen att hur olika aktörer förmår att omsätta dataskyddsförordningen i sina respektive verksamheter kommer att ha betydelse för hur väl Sverige förmår ta hand om potentialen och hantera riskerna med AI.**

Sedan 2018 har regeringen gett olika myndigheter en rad särskilda uppdrag för att främja Sveriges förmåga att använda AI, skapa och använda öppna data och fortsätta digitalisera den offentliga sektorn.

När integritetsskydd stått i fokus i svensk politik har det ofta varit i kontexten digital utveckling. Digitaliseringspolitiken har även på nationell nivå fått en tydligare prioritering de senaste åren, vilket märkts bland annat genom framtagandet av nationell digitaliseringsstrategi och en nationell inriktning för AI.

Digitaliseringspolitik omfattar bland annat arbete med att digitalisera offentlig förvaltning och att skapa goda förutsättningar för digital infrastruktur genom till exempel bredband, digital identitet och 5G. Andra delar av digitaliseringspolitiken handlar om att skapa goda förutsättningar för utveckling och användning av data och ny teknik som AI. Även arbete med att främja digital kompetens och digitalt ledarskap hör till området.

3.4.1 Digital trygghet – en viktig del av Sveriges digitaliseringsstrategi

Utgångspunkten för svensk digitaliseringspolitik de senaste åren har varit regeringens digitaliseringsstrategi *För ett hållbart Sverige – en digitaliseringsstrategi*, som beslutades i maj 2017. Det övergripande målet i digitaliseringsstrategin är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. I digitaliseringsstrategin bryts det övergripande målet ned i fem delmål:

- Digital kompetens
- Digital trygghet
- Digital innovation
- Digital ledning
- Digital infrastruktur.

Personlig integritet ingår i strategin som en uttalat viktig del av delmålet om digital trygghet.

Delmålet digital trygghet är viktigt för att alla individer och organisationer ska kunna känna tillit till att samhället är rustat för de risker som finns i en digital värld. Regeringen konstaterar i digitaliseringsstrategin att det krävs säkra digitala system, som värnar den personliga integriteten och att identifierade sårbarheter hanteras när människor och samhället i allt högre grad blir beroende av att teknik är uppkopplad och kommunicerbar via internet.

Delmålet digital trygghet har i sin tur konkretiserats ytterligare i sex olika områden:

- En digital identitet
- Höga krav på säkerhet
- Integritet i det digitala samhället
- Demokratin värnas i digitala miljöer
- En trygg och mobil arbetsmarknad
- Fungerande digitala marknader och trygga konsumenter.

I anslutning till att den nationella digitaliseringsstrategin antogs inrättade regeringen också ett digitaliseringsråd inom Regeringskansliet. Syftet med rådet är att bidra till bättre samordning och ett effektivt genomförande av regeringens strategiska arbete med digitalisering. Regeringen fattade i slutet av 2020 beslut om att förlänga digitaliseringsrådets uppdrag i ytterligare tre år.[51] Under 2018 inrättades också Myndigheten för digital förvaltning (DIGG), som tillsammans med Digitaliseringsrådet av regeringen beskrivs som viktiga delar i arbetet med utvecklingen och styrningen av digitaliseringspolitiken.[52]

51. https://www.regeringen.se/pressmeddelanden/12/fortsatt-arbete-for-digitaliseringsradet.

52. Prop 2020/21:1 *Budgetpropositionen för 2021*, utgiftsområde 22 Kommunikationer.

Under 2018 sammanställde Digitaliseringsrådet lägesbilder till regeringen om samtliga digitaliseringsstrategins delområden. I arbetet med lägesbilden om digital trygghet, som publicerades i oktober 2018, konstaterades att vissa områden var återkommande i intervjuer och workshops som Digitaliseringsrådet genomfört på temat digital trygghet. Dessa områden är bland annat att

Alla medborgare behöver grundläggande kunskaper – Viktiga områden där allmänhetens kunskap behöver öka är medie- och informationskunnighet (MIK), kunskap om hur personuppgifter används av olika företag och myndigheter samt informationssäkerhetskunskap.

Företag och organisationer behöver öka kompetensen om informations- och cybersäkerhet och det behöver ses som en strategisk verksamhetsfråga – Alla typer av organisationer behöver arbeta systematiskt med informationssäkerhet. Säkerhetsområdet behöver gå från att vara en teknikfråga till en strategisk verksamhetsfråga. Vid sidan om it-relaterade roller behöver ledningsfunktioner kunna ta ett större ansvar. För det krävs kompetens och kunskap. För detta behöver även säkerhetsfrågorna i högre grad integreras i de vanliga styrningsprocesserna, till exempel befintliga lednings- och ekonomistyrningssystem.

Avvägningar mellan den personliga integriteten och möjligheten att utveckla nya innovativa tjänster med data som en resurs behöver löpande hanteras – Många av de stora möjligheter som digitaliseringen medför uppstår på grund av, och är beroende av, de stora mängder data som samlas in från allmänheten till exempel vid användandet av digitala tjänster. Detta gäller både för det offentliga och det privata. Digitaliseringsrådet konstaterar att en av de största utmaningarna som följer av digitaliseringen ligger i att hitta en balans mellan användandet av insamlad personlig data och den personliga integriteten som inte hämmar utvecklingen och samtidigt gör att personers integritet värnas och att de känner tillit till de digitala miljöerna.

3.4.2 Särskilda insatser med fokus på AI och öppna data

Områden inom digitaliseringspolitiken som fått särskilt fokus rör AI och öppna data. I maj 2018 beslutade regeringen om en nationell inriktning för AI.[53] Syftet var att peka ut en övergripande färdriktning för AI-arbetet i Sverige och lägga en grund för kommande prioriteringar.

Inriktningen för AI knyter på ett tydligt sätt an till den övergripande digitaliseringsstrategin. Det är regeringens målsättning att Sverige ska vara ledande i att ta tillvara möjligheterna som användning av AI kan ge, med syftet att stärka både den svenska välfärden och den svenska konkurrenskraften.

Regeringen anger i den nationella inriktningen att Sverige behöver

- utveckla regler, standarder, normer och etiska principer i syfte att vägleda etisk och hållbar AI och användning av AI
- verka för svenska och internationella standarder och regelverk som främjar användning av AI och förebygger risker
- kontinuerligt se över behovet av digital infrastruktur för att tillvarata möjligheterna som AI kan ge
- fortsätta arbetet med att tillgängliggöra data som kan utgöra en samlad infrastruktur för att använda AI på områden där det tillför nytta
- fortsätta att ta en aktiv roll i EU:s arbete med att främja digitalisering och med att möjliggöra nyttan som användningen av AI kan medföra.

Centrala områden för att ta arbetet vidare är utbildning, forskning, innovation och användning samt ramverk och infrastruktur. När det gäller ramverk konstaterar regeringen att dataskyddsförordningen är en viktig del i ramverket för AI. Hur olika aktörer förmår att omsätta dataskyddsförordningen i sina respektive verksamheter kommer att ha betydelse för hur väl Sverige förmår ta hand om potentialen och hantera riskerna med AI.

Regeringen påtalar också att många av de regelverk och riktlinjer som Sverige har att förhålla sig till kommer från EU. För att Sverige ska kunna tillgodoräkna sig satsningar som görs inom EU behöver vi delta och ta en aktiv roll i det unionsgemensamma arbetet.

Sedan 2018 har regeringen också gett olika myndigheter en rad särskilda regeringsuppdrag för att främja Sveriges förmåga att använda AI och driva datadriven innovation.

53. Näringsdepartementet; *Nationell inriktning för artificiell intelligens*.

Bland annat har DIGG ett regeringsuppdrag att främja den offentliga förvaltningens förmåga när det gäller AI.[54] Statistiska centralbyrån (SCB), redovisade i november 2020 ett regeringsuppdrag att kartlägga användningen av AI samt analys av stora datamängder i Sverige.[55] Verket för innovationssystem (Vinnova) har bland annat haft i uppdrag att kartlägga hur väl AI och maskininlärning kommer till användning i svensk industri och det svenska samhället[56] samt att göra en förstudie för etableringen av digitala innovationshubbar utifrån kommissionens digitaliseringsstrategi. Det pågår också en stor mängd initiativ inom forskningsområdet.[57]

Ett antal initiativ har också tagits i Sverige som rör öppna data. Grundtanken är att data, genom att göras helt öppen eller tillgänglig inom olika digitala ekosystem, ska kunna användas av flera parter på ett enkelt och effektivt sätt. Därmed ökar också behovet av att kunna standardisera data på olika sätt – till exempel genom en sammanslutning av aktörer utvecklar gemensamma regelverk eller principer, genom gemensamma informationsmodeller eller genom att göra data maskinläsbar. Inom offentlig sektor används benämningen nationella grunddata om uppgifter som flera aktörer har behov av och som är viktiga i samhället, och ett ambitiöst arbete pågår för att underlätta utbytet av sådan data. I näringslivet har projektet *Digitala Stambanan* ett liknande syfte. Projektet utgår från tesen att dataströmmar i den nya ekonomin blir minst lika viktiga som fysiska flöden av råvaror och produkter. Projektet kartlägger behov och möjligheter med digitalt informationsutbyte i svensk industri.

Sverige saknar flera av de förvaltningsgemensamma lösningar för informationsutbyte som finns i jämförbara länder. Bristen på en nationell digital infrastruktur har lett till många olika myndighets- och sektorsspecifika lösningar, som skiljer sig från varandra. Mot denna bakgrund har DIGG fått ett regeringsuppdrag att leda arbetet med att skapa ett varaktigt, säkert och effektivt informationsutbyte inom och med den offentliga sektorn.[58] Uppdraget genomförs tillsammans med Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, MSB, Riksarkivet samt Skatteverket.

I och med att myndigheterna går mot att standardisera och bygga ut det förvaltningsgemensamma digitala informationsutbytet blir det extra viktigt att från början etablera ett gemensamt informationssäkerhetsarbete. Eftersom det är först i de aggregerade datamängderna som hela riskbilden framträder behöver arbetssätt utvecklas där organisationer gör konkreta risk- och konsekvensanalyser både tillsammans och var för sig. För att bygga en hållbar utveckling behöver organisationer redan från början bygga in dataskydd som standard och ta ansvar för säkerheten i produkterna, både vad gäller det enskilda bidraget och aggregerade konsekvenser av hur datan delas, förädlas och återanvänds i kommande led.

3.4.3 Digitalisering av offentlig sektor

Ett centralt område i digitaliseringspolitiken är digitaliseringen av offentlig sektor. Ett viktigt initiativ för att pröva och utvärdera former för samordnad och säker it-drift inom staten är Försäkringskassans tidsbegränsade uppdrag om att erbjuda it-drift för vissa statliga myndigheter.[59]

Regeringen har också tillsatt en särskild utredare med uppdrag att kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov tillgodoses.[60] Den så kallade it-driftsutredningen ska bland annat lämna förslag på mer varaktiga former för en samordnad statlig it-drift och tydliggöra de rättsliga förutsättningarna för att på ett säkert sätt kunna anlita privata leverantörer av it-drift. Uppdraget att kartlägga och analysera statliga myndigheters it-drift och den offentliga förvaltningens rättsliga förutsättningar för utkontraktering med bibehållen säkerhet, inklusive eventuella författningsförslag, redovisades den 15 januari 2021, medan förslagen till mer varaktiga former för samordnad statlig it-drift ska redovisas senast den 15 oktober 2021.

54. Myndigheten för digital förvaltning (DIGG) *Främja den offentliga förvaltningens förmåga att använda AI*. Delrapport i regeringsuppdrag I2019/01416/DF och I2019/01020/DF.

55. Statistiska centralbyrån (SCB) *Artificiell intelligens i Sverige*, 2020.

56. Vinnova slutrapport VR 2018:08 *Artificiell intelligens i svenskt näringsliv och samhälle - Analys av utveckling och potential*.

57. Se vidare avsnitt 7.

58. Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte. I2019/03306/DF, I2019/01036/DF (delvis), I2019/01361/DF (delvis), I2019/02220/DF.

59. I2019/02515/DF.

60. Dir. 2019:64 *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen*.

En central fråga i utredningen handlar om statliga myndigheters möjligheter att anlita privata leverantörers molntjänster. Risker med att statliga myndigheter använder molntjänster som tillhandahålls av privata leverantörer har tidigare bland annat belysts i Försäkringskassans vitbok om molntjänster i samhällsbärande verksamhet.[61] I vitboken ifrågasätter Försäkringskassan bland annat lämpligheten i att svenska myndigheter avhänder sig kontrollen över uppgifter i den verksamhet som vi benämner som samhällsbärande till privata företag eller andra länder. Till detta kommer olika säkerhetsrelaterade aspekter. Som exempel nämner Försäkringskassan i vitboken en ökad allmän sårbarhet, ökade risker för att obehöriga får tillgång till data samt svårigheter att säkerhetspröva personal och upprätta rättvisande risk- och sårbarhetsanalyser.[62]

EU-domstolens avgörande i Schrems II-målet,[63] där domstolen slår fast att det så kallade Privacy Shield-beslutet som möjliggör överföring av personuppgifter från EU/EES till USA inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA, har för många verksamheter ställt frågan om USA-baserade molntjänster på sin spets.

En tänkbar väg framåt kan vara en europeisk molntjänstinfrastruktur. Tyskland och Frankrike har inom ramen för projektet GAIA-X påbörjat ett arbete med en sådan infrastruktur. Projektet syftar bland annat till att stärka den europeiska digitala suveräniteten, att minska beroendet och inlåsningseffekter kopplat till enskilda kommersiella aktörer, att göra molntjänster mer attraktiva på bredare front, särskilt för små och medelstora företag samt att skapa ett europeiskt ekosystem för datadriven innovation. Från Sveriges håll har Skatteverket regeringens uppdrag att bevaka arbetet med projektet.[64]

Ett regeringsuppdrag under 2020 tar specifikt sikte på integritetsskydd och medborgarnas kontroll över data som finns hos offentlig sektor. Det handlar om ett uppdrag till Arbetsförmedlingen, E-hälsomyndigheten, DIGG och Skatteverket att genomföra en omvärldsanalys och ta fram ett koncepttest som visar hur individens möjligheter till insyn och kontroll över de data om individen som finns hos offentlig sektor, och i förlängningen även de data om individen som finns hos privat sektor, kan öka. Resultatet av uppdraget ska redovisas till Regeringskansliet senast den 1 juni 2021.

3.4.4 Digitaliseringspolitikens fortsatta inriktning

I budgetpropositionen för 2021 bedömde regeringen sammantaget att förutsättningarna är goda att nå det övergripande målet för digitaliseringspolitiken. Samtidigt, konstaterar regeringen, finns utmaningar som bidrar till att Sverige ännu inte är bäst i världen på att använda digitaliseringens möjligheter.[65]

För att nyttja AI och annan ny teknik på ett sätt som svarar mot målen på digitaliseringsområdet och invånarnas förväntan på den offentliga förvaltningen understryker regeringen att det behöver finnas en balans mellan innovation och grundlig analys för att säkerställa säker, resurseffektiv och ändamålsenlig användning av ny teknik. Data är en grundförutsättning för att kunna nyttja potentialen i AI och annan digital innovation. Arbetet behöver fortsätta med säker tillgång till öppna data och användningen av data som strategisk resurs, med respekt för regler om dataskydd och den personliga integriteten. Samverkan mellan olika aktörer behöver enligt regeringen främjas för att åstadkomma ett livskraftigt innovationsklimat, särskilt samordning av test- och experimentmiljöer.

Regeringen påtalar också att möjligheterna till digital och datadriven innovation kan förbättras genom ett effektivt utnyttjande av initiativ på europeisk nivå inom ramen för bland annat EU:s digitaliseringsstrategi, datastrategi och satsningar på AI och blockkedjor. Efter ett förslag från DIGG har regeringen aviserat att man under 2021 avser ta fram en nationell strategisk inriktning för data, som bland annat ska bidra till ett ökat utbud av och tillgänglighet till öppna data.

Regeringen avser också att vidta åtgärder i syfte att säkerställa långsiktighet och kontinuitet när det gäller att samlat följa upp och analysera hela samhällets digitalisering. Regeringen bedömer vidare att lagstiftningen kan behöva anpassas ytterligare för att ge ett tillräckligt stöd för en digital och datadriven offentlig förvaltning. Regeringen genomför också en satsning för att DIGG ska kunna vägleda och ge rättsligt stöd till den offentliga förvaltningen.

61. Försäkringskassan *Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt* Föräkringskassans diarienummer: 013428-2019.

62. Förslag till hantering av dessa problem lämnas i prop. 2019/20:201 *Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.*

63. Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18, “Schrems II”).

64. I2020/02296/DF.

65. Prop. 2020/21:1 *Budgetpropositionen för 2021* Utgiftsområde 22, avsnitt 4.5.1.

3.5 Sveriges integritetsskyddspolitik

På informations- och cybersäkerhetsområdet har en nationell strategi utarbetats och en rad åtgärder vidtagit. De sju myndigheterna i Samverkansgruppen för informationssäkerhet (SAMFI) ansvarar tillsammans för att genomföra den handlingsplan som finns kopplad till strategin.

Införandet av dataskyddsförordningen, brottsdatalagen och kompletterande regelverk är utan tvekan det mest betydelsefulla direkta integritetsskyddspolitiska arbetet under senare år.

Integritetskommittén lämnade 2017 ett antal förslag för att stärka den personliga integriteten. Ett antal förslag har realiserats, främst avseende informationssäkerhet och digitalisering av offentlig sektor. Bland de förslag som inte lett till åtgärder finns en rad branschspecifika åtgärder till exempel avseende uppförandekoder.

Sveriges integritetsskyddspolitik grundar sig på ett förstärkt grundlagsskydd för den personliga integriteten som infördes i 2 kap. 6 § andra stycket regeringsformen år 2011. Skyddet för den personliga integriteten i samband med behandling av personuppgifter har blivit mer uttalat under 2018 genom genomförandet av dataskyddsförordningen, brottsdatalagen och ett stort antal kompletterande regelverk på integritetsskyddsområdet. Ett omfattande arbete har också bedrivits med att stärka arbetet inom informationssäkerhets- och cybersäkerhetsområdet.

3.5.1 Informations- och cybersäkerhet

Ett viktigt område för att öka den digitala tryggheten handlar om informations- och cybersäkerhet. Givet att de aktörer som har störst kapacitet att utföra cyberangrepp utgörs av främmande makt är informations- och cybersäkerhetsfrågor sedan några år tillbaka en viktig del i svensk försvarspolitik.

Försvarsberedningen framhöll i sin rapport *Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025* att cybersäkerhetsfrågor får allt större betydelse i utrikes- och säkerhetspolitiken liksom för den nationella säkerheten.[66] De globala cyberdiskussionerna befinner sig i ett formativt skede, där frågorna spänner över ett brett fält med bland annat folkrätt, försvars- och säkerhetspolitik, mänskliga rättigheter och global utveckling.

Försvarsberedningen påtalade vidare att de mest skyddsvärda verksamheterna är beroende av funktionalitet och säkerhet inom andra verksamheter. Arbetet med skydd för de mest skyddsvärda verksamheterna kan därför inte bedrivas isolerat, utan måste ske koordinerat med det samlade arbetet med samhällets informations- och cybersäkerhet. Skyddsarbetet är ett gemensamt ansvar för hela samhället och måste enligt Försvarsberedningen bedrivas på central, regional och lokal nivå, hos myndigheter, företag och organisationer i Sverige. Den tekniska säkerheten behöver fortsatt stärkas samtidigt som hänsyn tas till att det i många fall är den mänskliga faktorn som ligger bakom incidenter eller utnyttjas vid angrepp. De åtgärder som vidtas för att exempelvis höja lägstanivån i informations- och cybersäkerhetsarbetet anses av Försvarsberedningen hänga samman med arbetet att skydda samhället mot avsiktliga cyberattacker.

Ett liknande anslag återfinns i den nationella säkerhetsstrategi som regeringen fattade beslut om 2017.[67] En robust cyberförsvarsförmåga framhålls som en viktig del av vår samlade ansats att stå emot riktade angrepp och försök till påverkan. I strategin framhålls att det, för att bemästra utmaningarna inom informations- och cybersäkerhetsområdet är viktigt att fortlöpande arbeta för att minska sårbarheter. Detta är en uppgift för alla aktörer i samhället, menar regeringen. Förmågan att förebygga, identifiera och hantera it-incidenter och antagonistiska attacker behöver förbättras inom alla samhällsviktiga funktioner. De mest skyddsvärda verksamheterna ska dessutom svara upp mot de krav som ställs i säkerhetsskyddslagstiftningen. Arbetet med att minska sårbarheter tar sin grund i verksamhetens risk- och sårbarhetsanalys och/eller säkerhetsanalys. En förutsättning för arbetet är en utvecklad samordning och samverkan mellan myndigheter och andra aktörer, för att identifiera vad som ska skyddas och vilka ytterligare säkerhetsåtgärder som behöver sättas in.

66. Ds 2017:66 *Motståndskraft Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025.*

67. Statsrådsberedningen; *Nationell säkerhetsstrategi*, 2017.

I oktober 2018 beslutade regeringen om en nationell strategi för samhällets informations- och cybersäkerhet.[68] I strategin framhålls att ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet bidrar till att säkerställa den fortsatta digitaliseringen av samhället och samtidigt hävda Sveriges säkerhet och nationella intressen. Ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet är också en viktig förutsättning för svensk tillväxt och konkurrenskraft, samt en nödvändighet för att näringslivet ska kunna utveckla och tillhandahålla konkurrenskraftiga varor och tjänster.

För att informationshantering och it-användning i samhället ska kunna utvecklas på ett tryggt och säkert sätt krävs att alla aktörer har en helhetssyn på informationssäkerhet, som ska vara en självklar och integrerad del i allt arbete på alla nivåer i samhället. Strategin innehåller sex strategiska prioriteringar:

- säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet
- öka säkerheten i nätverk, produkter och system
- stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter
- öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet
- öka kunskapen och främja kompetensutvecklingen
- stärka det internationella samarbetet.

Med utgångspunkt i den nationella strategin har regeringen gett sju myndigheter i uppdrag att gemensamt utarbeta en handlingsplan med aktiviteter för att genomföra strategin. Det handlar om myndigheterna i Samverkansgruppen för informationssäkerhet (SAMFI); MSB, Försvarets radioanstalt (FRA), Försvarets materielverk (FMV), Försvarsmakten, Post- och telestyrelsen (PTS), Polismyndigheten samt Säkerhetspolisen. Handlingsplanen spänner över åren 2019–2022 och SAMFI-myndigheterna har regeringens uppdrag att fortsätta arbeta med åtgärderna i handlingsplanen.

Regeringen har också gett MSB ett antal särskilda regeringsuppdrag avseende informationssäkerhet. Det har bland annat handlat om riktade utbildningsinsatser till statliga myndigheter, kommuner, regioner och länsstyrelser för att höja nivån på informationssäkerhetsarbetet i offentlig sektor samt att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Myndigheten har också haft i uppdrag att bidra till att öka allmänhetens kunskap om informationssäkerhet, vilket bland annat resulterat i den nationella kampanjen *Tänk säkert!*

68. Skr. 2016/17:213 *Nationell strategi för samhällets informations- och cybersäkerhet.*

MSB har också en central roll i arbetet med implementeringen av NIS-direktivet i Sverige.[69] Lagen ställer krav på leverantörer av samhällsviktiga tjänster inom sju utpekade sektorer samt, under vissa förutsättningar, leverantörer av digitala tjänster. De sju sektorerna för samhällsomfattande tjänster är energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. För var och en av sektorerna finns en utpekad tillsynsmyndighet. MSB:s uppdrag på området innefattar bland annat föreskriftsrätt och samordning för de olika sektorsspecifika tillsynsmyndigheterna i syfte att säkerställa en effektiv och likvärdig tillsyn. MSB är också mottagare av incidentrapporter.

Vidare har regeringen beslutat att ett nationellt cybersäkerhetscentrum ska startas och gett FRA, Försvarsmakten, MSB och Säkerhetspolisen i uppdrag att tillsammans vidta förberedande åtgärder. Det nationella cybersäkerhetscentret ska stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska cybersårbarheterna. Det ska ge ett utvecklat och samordnat stöd om hur privat och offentlig sektor kan skydda sig mot cyberattacker.

3.5.2 Integritetsskyddspolitiken i Sverige – dataskyddsreformen har implementerats

I Sverige har integritetsskyddspolitiken främst fått tydliga uttryck genom införandet av dataskyddsförordningen och övriga regelverk på dataskyddsområdet. Bland annat har kompletterande nationell lagstiftning genomförts genom dataskyddslagen, men på området har också ett EU-direktiv rörande personuppgiftsbehandling i brottsbekämpande verksamhet implementerats genom införandet av brottsdatalagen. I samband med införandet av dataskyddsförordningen, dataskyddslagen och brottsdatalagen genomfördes också omfattande ändringar och anpassningar i nationell kompletterande sektorsspecifik lagstiftning.[70] Detta innebär att regeringen har säkerställt att grundläggande regelverk finns på plats som har integritetsskyddsaspekterna i fokus.

Vilka krav regelverket ställer på behandling av data beskrivs övergripande i kapitel 4 och något mer fördjupat i en bilaga till rapporten.

69. Som en del i EUs strategi på cybersäkerhetsområdet antogs NIS-direktivet (EU Network and Information Security Directive) 2016. Det var ett av de första initiativen för att skapa en EU-övergripande reglering, i syfte att öka cybersäkerheten över hela unionen. Eftersom det är ett direktiv har det implementerats i resp. medlemsstat genom nationell lagstiftning, i Sverige genom lag (2018:1174) och förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

70. Det kan på sina håll fortfarande finnas bristande harmonisering mellan medlemsstaternas nationella kompletterande lagstiftning. Svenskt näringsliv pekar på detta som ett problem i sin skrift ”*Vad är fel med GDPR?*”.

3.5.3 Regeringen har agerat på ett antal av Integritetskommitténs förslag från 2017

Inom ramen för integritetsskyddspolitiken har regeringen också agerat på ett antal förslag som tidigare lämnats. Integritetskommittén lämnade i sitt slutbetänkande 2017[71] totalt 36 förslag på åtgärder som kommittén ansåg kunde stärka skyddet för den personliga integriteten. För ungefär hälften av kommitténs förslag har någon form av åtgärder vidtagits, även om det inte nödvändigtvis är exakt i enlighet med kommitténs förslag. Flest åtgärder har vidtagits inom områdena informationssäkerhet och e-förvaltning.

3.5.3.1 Förslag som har genomförts

Flera av Integritetskommitténs förslag om informationssäkerhet har genomförts, bland annat i delar som avser uppdrag till MSB. Bland annat föreslogs att MSB skulle få ett tillsynsuppdrag avseende statliga myndigheters informationssäkerhet, att MSB skulle få uppdraget att utveckla en styrmodell för informationssäkerhetsarbete i staten samt följa upp statliga myndigheters informationssäkerhetsarbete. Som redovisats ovan har MSB också fått ett antal regeringsuppdrag som rör informationssäkerhet.

Vidare uppmanade Integritetskommittén att regeringen borde följa upp Riksrevisionens rekommendationer avseende kompetens och metod för utredning av it-brott. Regeringen har också gett Polismyndigheten i uppdrag att ta fram en långsiktig plan för att säkerställa att rätt kompetens finns att tillgå i verksamheten för att utreda it- brott.[72]

Integritetskommittén lämnade också flera förslag rörande e-förvaltning, varav merparten genomförts. Ett av förslagen handlade om att den myndighet som får det samlade ansvaret för den offentliga förvaltningens digitalisering – vilket kom att bli DIGG – i sin instruktion bör ha särskilt uttalat att myndigheten ska främja skyddet av den personliga integriteten. Av instruktionen för DIGG framgår att myndigheten ska bedriva arbetet med digitalisering av den offentliga förvaltningen på ett sätt som säkerställer skyddet av säkerhetskänslig verksamhet och informationssäkerhet i övrigt samt skyddet av den personliga integriteten.[73] Även i flera av myndighetens regeringsuppdrag framhålls att särskilt fokus ska läggas på säkerhet, informationssäkerhet, sekretess och integritetsskydd.

I enlighet med kommitténs förslag har regeringen också utarbetat ett lagförslag om tystnadsplikt för leverantörer av molntjänster och andra personuppgiftsbiträden.[74] Riksdagen har antagit regeringens förslag och lagändringen trädde ikraft den 1 januari 2021.[75] Vidare har regeringen, i enlighet med vad som ursprungligen föreslogs av Statens Servicecenter och tillstyrktes av Integritetskommittén, tillsatt en utredning för att utreda förutsättningarna för inrättandet av en statlig molntjänst som den offentliga förvaltningen ska kunna använda sig av (it-driftsutredningen som beskrivs ovan).

3.5.3.2 Förslag som inte har genomförts

En rad av kommitténs förslag rörde uppförandekoder i olika branscher. Kommittén föreslog att regeringen bör initiera och stödja framtagandet av uppförandekoder inom konsumentområdet, skolan, hälso- och sjukvården, arbetslivet och e-förvaltningen. Mer specifikt lämnade kommittén förslag på regeringsuppdrag till bland annat Konsumentverket, Skolverket, E-hälsomyndigheten och Arbetsmiljöverket för att initiera och stödja arbetet med uppförandekoder i olika branscher. Några sådana regeringsuppdrag har inte lämnats.

Generellt när det gäller uppförandekoder kan konstateras att IMY endast fått in ett fåtal ansökningar om godkännande av uppförandekoder sedan maj 2018 och att ingen avser de föreslagna branscherna eller sektorerna. Det kan också konstateras att främjandet av instrument för att säkerställa integritetsskyddet, bland annat uppförandekoder, är ett av fokusområdena för kommissionens fortsatta utvärdering av dataskyddsförordningens genomförande.

Kommittén lämnade också ett antal branschspecifika förslag där åtgärder inte vidtagits. Förslagen handlade till exempel om att utreda en lagreglerad tystnadsplikt för försäkringsföretag och deras anställda avseende personuppgifter och reglering av ett teknikoberoende skydd för den enskildes integritet vid kreditupplysning.

Vidare menade Integritetskommittén att regeringens digitala strategier bör kompletteras med uttryckliga mål som avser den personliga integriteten. Målet, ansåg kommittén, bör vara att Sverige inte bara ska vara bäst i världen på att utnyttja digitaliseringens möjligheter, utan också världsledande på att skydda den personliga integriteten. Något sådant mål har inte fastställts.

Integritetskommittén konstaterade också att det finns ett behov av att i högre grad integrera arbetet med att skydda den personliga integriteten med det traditionella informationssäkerhetsarbetet.

71. SOU 2017:52 *Så stärker vi den personliga integriteten.*
72. Ju2020/00378/PO.
73. Förordning (2018:1486) med *Instruktion för Myndigheten för digital förvaltning*, 8 §.
74. Prop. 2019:20:201 *Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.*
75. Lag (2020:914) om *Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.*

Ett förslag som inte heller genomförts rör inrättandet av ett kompetenscenter för frågor som rör anskaffning och användning av externa it-tjänster. Upphandlingsmyndigheten tillhandahåller dock generellt stöd och vägledning för upphandling och avtalsförvaltning och MSB har tagit fram en vägledning för att upphandla informationssäkert.[76] Integritetskommittén menade att ett dedikerat kompetenscenter skulle kunna bidra till att den offentliga förvaltningen blir bättre kravställare i upphandlingar, bland annat vad gäller kraven på inbyggt dataskydd och dataskydd som standard.

3.5.3.3 Förslag som har rört tydligare reglering i lag

Även när det rör lagreglering lämnade Integritetskommittén förslag som inte har genomförts. Ett inledande konstaterande från kommittén var till exempel att det är otillfredsställande att regeringsformens skydd av den personliga integriteten tillämpas på så olika sätt av utredningar, myndigheter och inom Regeringskansliet.[77] Kommittén menade att mycket tid skulle kunna sparas i lagstiftningsprocessen om det framgick tydligare i utredningar vilka avvägningar rörande den personliga integriteten som ett lagstiftningsförslag aktualiserar. Mot denna bakgrund föreslog kommittén en ändring i kommittéförordningen (1998:1474) med innebörden att om förslagen i ett betänkande har betydelse för den personliga integriteten i de fall som avses i 2 kap. 6 § andra stycket regeringsformen, ska konsekvenserna anges i betänkandet. Något sådant krav har inte förts in i kommittéförordningen, även om det i vissa enskilda utredningsdirektiv specifikt anges att utredaren särskilt ska beskriva vilka konsekvenser de förslag som lämnas har för den personliga integriteten.

Utredningen föreslog därtill att regeringen bör utvärdera, utveckla och vid behov uppdatera IMY:s vägledning för integritetsanalys, vilket inte genomförts. Ett arbete pågår dock inom IMY med att uppdatera vägledningen och den avses publiceras första halvåret 2021.

Inom vissa områden menade Integritetskommittén att det saknas viktig reglering om hur personuppgifter ska hanteras, vilket lämnar de personuppgiftsansvariga i ett svårt läge. Kommittén menade till exempel att det behövs en ny socialtjänstdatalag som reglerar den personuppgiftsbehandling som sker inom socialtjänsten. En sådan utredning har också tillsatts.[78]

Kommittén konstaterade att digitalisering och personlig integritet är ett område som förtjänar större uppmärksamhet i forskningen, både för att höja kunskapsnivån men också för att bidra till att finna lösningar av tekniska och legala utmaningar. De föreslog därför att regeringen skulle ge Vetenskapsrådet i uppdrag att fördela anslag till tvärvetenskaplig forskning på temat, samt att Vinnova ges ett uttalat uppdrag att främja projekt som involverar integritetsstärkande teknik och arbetssätt samt att upplysa om dataskyddsförordningen i sitt arbete.

Någon direkt koppling till Integritetskommitténs förslag kan inte spåras, men forskning inom digital utveckling och personlig integritet bedrivs vid flera lärosäten i Sverige. Exempel på pågående forskning ges i kapitel 7 i rapporten.

Vinnova fick också i december 2019 ett regeringsuppdrag att stödja offentliga aktörer i deras arbete med regel- och policyutveckling. Vinnova ska tillhandahålla stöd till offentliga aktörer, däribland regelgivande myndigheter, för att stärka deras förmåga att proaktivt arbeta med regel- och policyutveckling. Vinnova är också en av finansiärerna till AI Sweden, en paraplyfunktion som ska utgöra en samlande kraft för tillämpad AI för Sverige. En del av den nationella stödfunktionens uppdrag handlar om att stödja arbetet med rättsutveckling, där frågor som rör dataskyddsförordningen utgör en viktig del.

För att klargöra vilket anslag, vilka resurser och vilka kompetenser som dataskyddsmyndigheten behöver de närmaste åren, ansåg Integritetskommittén att regeringen bör ge Statskontoret i uppdrag att utföra en myndighetsanalys av IMY. En sådan myndighetsanalys har utförts och presenterades av Statskontoret i juni 2020.[79]

Andra förslag på tydligare reglering har inte åtgärdats. Det rör till exempel nya integritetsstärkande regler i patientdatalagen, reglering av medborgarprofilering, utredning av ett utökat sekretesskydd för uppgifter om elever i skolans it-system samt lagreglering av vissa integritetskänsliga spaningsmetoder. Dessa frågor har fortsatt hög aktualitet.

76. MSB 1177; *Upphandla informationssäkert – en vägledning*.

77. 2 kap. 6 § andra stycket regeringsformen.

78. SOU 2020:47 *Hållbar socialtjänst – En ny socialtjänstlag* (innehåller förslag till lag om socialtjänstdataregister).

79. Statskontorets rapport 2020:14 *Myndighetsanalys av Datainspektionen.*

4. Vilka krav ställer regelverket på skydd för personuppgifter?

Skyddet för våra personuppgifter har förstärkts väsentligt genom dataskyddsreformen. I det här kapitlet ges en kort bakgrund till dataskyddsförordningen och en sammanfattning av de viktigaste förändringarna som lagstiftningen innebar. Vi gör också en kort genomgång av det dryga tiotal domar som kommit från EU- domstolen sedan dataskyddsförordningen trädde i kraft.

En mer utförlig redovisning av de rättigheter och skyldigheter som regleras i dataskyddsförordningen återfinns i en bilaga till denna rapport.



4.1 Från direktiv till förordning

Ett viktigt syfte med införandet av dataskyddsförordningen var att möta den snabba tekniska utvecklingen och ökande insamlingen och delningen av personuppgifter.

Till skillnad från det tidigare dataskyddsdirektivet gäller dataskyddsförordningen direkt i medlemsstaterna och förordningen är primär rätt, vilket innebär att all nationell lagstiftning ska anpassas till förordningen.

Ett första stort steg på integritetsskyddstrappan togs 1973 då datalagen infördes. Sverige var först ut med att inrätta en tillsynsmyndighet på området och den 1 juli 1973 inrättades Datainspektionen. Nästa stora steg togs 1998 då dataskyddsdirektivet infördes, och genom direktivet togs det första gemensamma steget i syfte att åstadkomma en harmoniserad tillämpning inom EU.[80] Direktivet infördes i svensk rätt genom personuppgiftslagen (1998:204).

Mot bakgrund av bland annat den snabba tekniska utvecklingen och den omfattande insamlingen och delningen av personuppgifter bedömdes att det krävs en stark och mer sammanhängande ram för dataskyddet inom unionen, uppbackad av ett kraftfullt tillsynsarbete. Efter ett långvarigt förhandlingsarbete infördes dataskyddsförordningen den 25 maj 2018. Förordningen gäller nu direkt som lag i samtliga EU:s medlemsländer.[81] I anslutning till detta arbetades en stor mängd regelverk fram och anpassningar har som tidigare nämnts skett i stor omfattning av sektorsspecifika regelverk.

En av grunderna för att stärka enskildas rättigheter genom en förordning vara att det fortfarande fanns brister i hur länderna implementerat och tolkat direktivet, vilket lett till rättsosäkerhet och återstående betydande risker för enskilda individer, särskilt vid användning av internet. Genom förordningen avsågs en konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter säkerställas i hela unionen.

Det som är nytt efter att dataskyddsförordningen infördes är att den idag är det primära regelverket när det gäller personuppgiftsbehandling. Personuppgiftslagen var subsidiär i förhållande till andra bestämmelser, det vill säga den gällde bara om det inte fanns andra bestämmelser på området.[82] Idag måste all personuppgiftsbehandling uppfylla kraven enligt dataskyddsförordningen. Nationell rätt ska ha anpassats till förordningen och utgör kompletterande lagstiftning.[83] Det räcker således inte att uppfylla nationella föreskrifter och om det uppstår konflikt mellan regelverk går dataskyddsförordningen före.

Dataskyddsförordningen innehåller 99 artiklar och 173 beaktandesatser. Detta utgör regelverket i sin helhet och ytterligare förarbeten saknas. I beaktandesatserna, där syftet bakom regleringen beskrivs, betonas att den tekniska utvecklingen och de nya möjligheter som idag finns att ta tillvara digitaliseringens möjligheter behöver balanseras med ett effektivt integritetsskydd.

Av beaktandesatserna framgår vidare att ett effektivt skydd av personuppgifter över hela unionen förutsätter att de registrerades rättigheter förstärks och specificeras, att de personuppgiftsansvarigas och personuppgiftsbiträdenas skyldigheter vid behandling av personuppgifter klargörs, att det finns likvärdiga befogenheter för övervakning, att det säkerställs att reglerna för skyddet av personuppgifter efterlevs samt att sanktionerna för överträdelser är likvärdiga i medlemsstaterna.

80. Direktiv 94/95/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter antogs 1995 och implementerades i nationell rätt genom personuppgiftslagen 1998.

81. Ett nytt direktiv på det brottsbekämpande området genomfördes för Sveriges vidkommande per den 1 augusti 2018 genom brottsdatalagen (2018:1177) och brottsdataförordningen (2018:1202).

82. I 2 § personuppgiftslagen angavs att om det i en annan lag eller i en förordning finns bestämmelser som avviker från denna lag, ska de bestämmelserna gälla.

83. Ett område där detta möjligen inte uppfattas som tillräckligt klart är kamerabevakning – även om man har fått tillstånd till bevakning behöver bevakningen uppfylla regleringen i GDPR. Detta gäller också om verksamheten inte behöver tillstånd – dataskyddsförordningen gäller för bevakningen.

4.2 Förstärkta rättigheter och skärpta skyldigheter

Genom dataskyddsförordningen har *enskildas rättigheter stärkts*. Samtidigt innebär förordningen på en rad områden *skärpta skyldigheter för alla verksamheter* som hanterar personuppgifter.

Skyldigheterna för verksamheter som behandlar personuppgifter utgår från förordningens sex *grundläggande principer* och att det krävs en *rättslig grund* för att få behandla personuppgifter. Är inte de grundläggande principerna beaktade eller om rättslig grund saknas kan man utgå från att personuppgiftsbehandlingen inte är laglig.

Centralt för att skapa den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden är att enskilda individer har kontroll över sina egna personuppgifter. Dataskyddsförordningen innebär på en rad områden stärkta rättigheter för enskilda.

Det handlar bland annat om rätten till (klar och tydlig) information, rätten att få personuppgifter rättade, raderade eller överförda, rätten att få göra invändningar (till exempel om uppgifter används för direktmarknadsföring) och rätten att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling.

Den enskildes rättigheter är långtgående och förutsätter att den som hanterar personuppgifter har ordning och reda och kan härleda personuppgifter som kan kopplas till en viss individ samt också rutiner och processer för att ge enskilda den insyn och kontroll över sina uppgifter de har rätt till.

Enskildas rättigheter balanseras med utökade och omfattande skyldigheter för den som behandlar personuppgifter, oftast personuppgiftsansvariga men även biträden till dessa har fått uttalade skyldigheter. Kraven på en personuppgiftsansvarig är bland annat att man vid behandling av personuppgifter följer förordningens sex grundläggande principer,[84] som rör

- **Laglighet, korrekthet och öppenhet** – uppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade
- **Ändamålsbegränsning** – uppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (den så kallade finalitetsprincipen)
- **Uppgiftsminimering** – uppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas
- **Korrekthet** – uppgifter ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål
- **Lagringsminimering** – uppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.
- **Integritet och konfidentialitet** – uppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet – inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse – med användning av lämpliga tekniska eller organisatoriska åtgärder.

Därutöver anges principen om *ansvarsskyldighet* – den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna efterlevs.

Är inte de grundläggande principerna beaktade eller om rättslig grund saknas kan man utgå från att man inte uppfyller de närmare förskrifterna i förordningen och att personuppgiftsbehandlingen därmed inte är laglig.[85] Följs de grundläggande principerna har man också till stora delar säkerställt att enskildas rättigheter tillgodoses.

84. Artikel 5.1 (a–f) dataskyddsförordningen.
85. Rättsliga grunder regleras i artikel 6 och, för känsliga personuppgifter, dessutom i artikel 9 i dataskyddsförordningen.

För att en personuppgiftsbehandling ska vara laglig krävs att den ansvariga verksamheten säkerställt att det finns en *rättslig grund* för att behandla uppgifterna. Rättslig grund kan utgöras av (ett frivilligt och uttryckligt) samtycke. Andra rättsliga grunder kan handla om att behandlingen är nödvändig för att verksamheten ska kunna uppfylla en rättslig förpliktelse, ett avtal, att skydda ett (för den enskilde) vitalt intresse eller utföra en uppgift av allmänt intresse. En rättslig grund kan också vara att verksamheten gjort en intresseavvägning – där verksamhetens intresse av att få behandla uppgifterna bedömts väga tyngre än den enskildes intresse.

Att säkerställa att de grundläggande principerna uppfylls och att det finns en rättslig grund förutsätter i grunden ett kontinuerligt och systematiskt arbete med att säkerställa att man har kontroll över vilka uppgifter som hanteras, varför, på vilket sätt och av vem.

Verksamheter som hanterar personuppgifter är också skyldiga att vidta *säkerhetsåtgärder* och genomföra *konsekvensbedömningar* för att bedöma de risker som uppstår genom att personuppgifter behandlas. Om behandlingen innebär en hög risk för enskildas integritet ska *förhandssamråd* begäras med tillsynsmyndigheten. Myndigheten kan då antingen lämna råd eller förbjuda behandlingen.

För att säkerställa ett kraftfullt tillsynsarbete har tillsynsmyndigheterna fått utökade och mer långtgående korrigerande befogenheter där sanktionsavgifter numera är huvudregel vid överträdelse av förordningen. Sanktionsavgifterna är höga och kan vid överträdelser som bedöms särskilt allvarliga för privata aktörer uppgå till 20 miljoner euro eller 4 procent av företagets globala årsomsättning, beroende på vilket belopp som är högst.[86] För myndigheter kan sanktionsavgiften enligt svensk rätt som mest uppgå till 10 miljoner kronor.[87]

I syfte att säkerställa ett enhetligt och harmoniserat genomförande av dataskyddsförordningen har som beskrevs i kapitel 3 inrättats ett särskilt organ inom EU, Europeiska dataskyddsstyrelsen (EDPB), med ett självständigt mandat som sträcker sig långt.[88]

4.3 EU-domstolens tolkning av förordningen

Sedan GDPR trädde i kraft har EU-domstolen meddelat ett tiotal domar som rör integritetsskydd. Genomgående kan konstateras att domstolen ofta gjort en strikt tolkning av dataskyddsreglerna.

Ett av de mer uppmärksammade målen rör det så kallade Schrems II-ärendet från juli 2020 där domstolen klargör vad som gäller vid *överföring till tredje land*. EU-domstolen slog i ärendet fast att Privacy Shield-avtalet mellan EU och USA inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA, vilket i praktiken innebär att många dataöverföringar mellan Europa och USA blev olagliga.

Andra avgöranden från EU-domstolen behandlar bland annat hur och när *samtycke* kan användas som rättslig grund för att vara giltigt, hur det så kallade *privatundantaget* ska tolkas, hur *personuppgiftsansvaret ska tolkas* när företag eller andra organisationer driver konton på Facebook eller andra sociala plattformar och vilka skyldigheter *sökmotorer* har när det gäller rätten att få information borttagen.

I detta avsnitt ges en kortfattad beskrivning av den praxis som hittills utvecklats av EU-domstolen när det gäller integritetsskydds- och dataskyddsfrågor. Domstolen har sedan den 25 maj 2018 meddelat ett tiotal domar på området. Sammanställningen ger en bild av hur domstolen ser på integritetsskyddet. Noterbart är att domstolen ofta gjort en strikt tolkning av dataskyddsreglerna.

86. Artikel 58.2 (f), artikel 83 dataskyddsförordningen.
87. 6 kap. 2 § dataskyddslagen.
88. Artikel 69–76 dataskyddsförordningen, se vidare avsnitt 3.2.1–2.

Ett av de mer uppmärksammade målen rör EU-domstolens underkännande av Privacy Shield där domstolen klargör vad som gäller vid överföring till tredje land (Schrems II).[89] EU-domstolen slår i målet i juli 2020 fast att Privacy Shield-avtalet mellan EU och USA inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA. Domstolen ansåg att kommissionens beslut om standardavtalsklausuler är fortsatt giltigt och att sådana kan användas vid överföring till länder utanför EU, men att det kan behövas ytterligare skyddsåtgärder. Så är fallet om mottagarlandet genom sin lagstiftning eller praxis inte kan anses tillförsäkra en i allt väsentligt likvärdig skyddsnivå för uppgifterna som inom EU. Domstolen uttalar också tydligt en förväntan på tillsynsmyndigheterna att granska de klagomål som kommer in, i vart fall i gränsöverskridande ärenden, då det är grundläggande för att kunna tillförsäkra enskilda deras grundläggande rättigheter.

4.3.1 Flera mål rör samtycke, personuppgiftsansvar och privatundantagets gränser

Ett par ärenden förtydligar vad som gäller för att använda samtycke som rättslig grund för personuppgiftsbehandlingen. I det så kallade Planet49-målet[90] uttalade domstolen att ett samtycke måste lämnas genom en otvetydig viljeyttring vilket förutsätter ett aktivt beteende från den som lämnar sitt samtycke. Att man måste ”avmarkera” en på förhand ikryssad ruta för att vägra sitt samtycke utgör därmed inte ett giltigt samtycke. I fallet Orange Romania[91] förtydligade domstolen att ett samtycke inte är giltigt, när villkoren i avtalet kan vilseleda den enskilde individen om möjligheten att ingå avtalet även om han eller hon vägrar att ge sitt samtycke. Ett samtycke är inte heller giltigt när den personuppgiftsansvarige på ett otillbörligt sätt påverkar möjligheten att fritt motsätta sig behandlingen genom att kräva att individen fyller i ytterligare ett formulär för att ge uttryck för denna vägran.

Flera mål har rört personuppgiftsansvaret och dess gränser. I fallet Wirtschaftsakademie[92] angav domstolen att enbart den omständigheten att någon använder sig av ett socialt nätverk inte innebär att en användare blir medansvarig för detta nätverks behandling av personuppgifter. Genom att skapa en sida och på den ge Facebook möjlighet att placera kakor hos en person som besöker sidan, oavsett om denne har ett konto hos Facebook, ansågs administratören dock ha medverkat till att fastställa ändamålen och medlen för behandlingen och betraktades därför som gemensamt personuppgiftsansvarig med Facebook för behandlingen.

I Fashion ID-målet[93] konstaterades att genom att integrera ett insticksprogram från ett socialt nätverk på sin webbplats, som översänder webbplatsbesökarnas personuppgifter till det sociala nätverket, hade företaget tillräckligt stort inflytande över behandlingen för att bestämma att den ska inledas eller avslutas och var därmed gemensamt personuppgiftsansvarigt med det sociala nätverket för den del av personuppgiftsbehandlingen som utfördes genom insticksprogrammet. I bedömningen togs även hänsyn till att företaget hade ett ekonomiskt intresse i att behandlingen utfördes.

Domstolen har slutligen konstaterat att ett utskott i ett delstatsparlament är personuppgiftsansvarig, i den mån utskottet ensamt eller tillsammans med andra fastställer ändamålen och medlen för behandlingen.[94]

Ett par fall har rört det så kallade privatundantagets gränser. Insamling av personuppgifter som medlemmar i ett religiöst samfund ägnar sig åt inom ramen för sitt predikoarbete genom dörrknackning och senare behandlar omfattas inte av privatundantaget.[95] För att privatundantaget ska vara tillämpligt får inte föras register, särskilda förteckningar eller andra arrangemang som medger sökning. Vidare konstateras att samfundet ska anses ansvarigt för behandlingen av personuppgifter som samlats in av dess medlemmar. EU-domstolen har också i ett mål bekräftat tidigare praxis att privatundantaget inte omfattar spridning av personuppgifter på internet till ett obegränsat antal personer. Inspelning av ett videoklipp på en polisstation som publicerats på internet ansågs vara en form av personuppgiftsbehandling där privatundantaget inte var tillämpligt.[96]

89. Dom av den 16 juli 2020, Facebook Ireland och Schrems, C-311/18, EU:C:2020:559.
90. Dom av den 1 oktober 2019, Planet49, C-673/17, EU:C:2019:801.
91. Dom av den 11 november 2020, Orange Romania, C-61/19, EU:C:2020:901.
92. Dom av den 5 juni 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388.
93. Dom av den 29 juli 2019, Fashion ID, C-40/17, EU:C:2019:629.
94. Dom av den 09 juli 2020, Land Hessen, C-272/19, EU:C:2020:535.
95. Dom av den 10 juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551.
96. Dom av den 14 februari 2019, Buivids, C-345/17, EU:C:2019:122.

Domstolen förtydligade också att behandling av personuppgifter uteslutande för journalistiska ändamål sker om behandlingen endast syftar till att sprida information, åsikter eller idéer till allmänheten. Undantaget för journalistiska ändamål ska dock endast tillämpas om det är nödvändigt för att förena rätten till skydd för personuppgifter med rätten till yttrandefrihet.

4.3.2 Mål som rör sökmotorer

Ett par avgöranden rör sökmotorer. EU-domstolen konstaterade i ett mål rörande Google[97] att det vid begäran om borttagande (rätten att bli bortglömd) inte finns någon automatisk skyldighet att göra sökträffar otillgängliga globalt. Vid borttagning av sökträffar är dock sökmotorleverantörerna ansvariga att vidta åtgärder som ska hindra eller i betydande utsträckning avhålla andra internetanvändare från att komma åt de aktuella länkarna genom att söka på personens namn. Det omfattar att ta bort länkar från alla versioner av sökmotorn som finns på EU-medlemsstaternas toppdomäner, såsom.se, .fr eller. dk. Däremot behöver länkar inte per automatik göras otillgängliga vid sökningar från tredje länder.

EU-domstolen konstaterade samtidigt[98] att förbudet mot behandling av känsliga personuppgifter och uppgifter om lagöverträdelser är tillämpligt för en sökmotorleverantör i sin egenskap av personuppgiftsansvarig. Behandling av känsliga personuppgifter kan ibland vara motiverad, men en registrerad kan ha rätt att få sökträffar borttagna ändå. Om en sökträff innehåller känsliga personuppgifter så kan personuppgiftsbehandlingen utgöra ett synnerligen allvarligt ingrepp i den personliga integriteten, vilket ska vägas in i bedömningen.

Det finns också några avgöranden som avser lagstiftning som angränsar till dataskyddslagstiftningen.[99]

---

97. Dom av den 24 september 2019, Google, C-507/17, EU:C:2019:772.

98. Dom av den 24 september 2019, GC m.fl., C-136/17, EU:C:2019:773.

99. Till exempel har EU-domstolen förtydligat sin praxis gällande ingrepp i den enskildes rätt till skydd av elektronisk kommunikation (dom av den 2 oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788) och möjligheterna att älägga en leverantör av elektroniska kommunikationstjänster att utföra lagring av trafik- och lokaliseringsuppgifter i syfte att bekämpa brott i allmänhet eller för att skydda nationell säkerhet (dom av den 6 oktober 2020, Privacy International, C-623/17, EU:C:2020:790 och dom av den 6 oktober 2020, La Quadrature du Net m.fl., förenade målen C-511/18, C-512/18 och C-520/18, EU:C:2020:791).

5. Digitalisering och teknikutveckling



Detta kapitel är rapportens kärna, här beskrivs digitaliseringen och teknikutvecklingen de senaste åren uppdelat på sammanlagt sexton olika teknikutvecklingsområden. Vissa avsnitt är mer fördjupade, medan andra innehåller mer övergripande beskrivningar. Vi ger exempel på vilka nyttor och användningsområden som finns med tekniken, men också vilka integritetsrisker.

Vi har delat upp teknikutvecklingsområdena i teknik som påverkar olika delar av personuppgifternas livscykel - där uppgifter samlas in, bearbetas och analyseras, lagras, säkras, transporteras och förstörs. Kapitlet inleds med ett avsnitt om tempot i teknikutvecklingen.

5.1 Hastigheten i teknikutvecklingen är exponentiell

Hastigheten i teknikutvecklingen är exponentiell, vilket förenklat innebär att kapaciteten fördubblas ungefär vartannat år.

Genombrott inom ett teknikområde skapar förutsättningar för framsteg inom andra områden. Att teknik som till exempel beräkningskraft, uppkopplingshastighet, lagringsutrymme och kamerasensorer utvecklas exponentiellt innebär sammantaget att de kommande 100 åren beräknas komma att motsvara 20 000 år av teknikutveckling.

Teknikutvecklingen kan också illustreras med antalet publicerade patent. Under de tre senaste åren har antalet patent som avser maskininlärning, molnlösningar, biometri, Internet of things (IoT) och big data fördubblats. Störst är ökningen inom IoT där en fyrdubbling skett 2019 jämfört med 2016.

Den tekniska utvecklingen och implementeringen av ny teknik går mycket snabbt framåt. Genombrott inom ett teknikområde skapar förutsättningar för framsteg inom andra områden och sammantaget ändras förutsättningarna kontinuerligt. Ett konkret exempel på hur utvecklingen inom olika teknikområden förstärker varandra är att intresset för AI tagit ordentlig fart tack vare tillgången på stora datamängder (big data) i kombination med ökad lagringskapacitet i molnet och ökad processorkraft. Med ökad användning av AI ökar i sin tur efterfrågan på data ytterligare, eftersom AI-baserade system behöver stora mängder relevant information att lära av. Innovation möjliggör nya innovationer och skapar ett slags ”ränta på ränta-effekt” som accelererar tempot i teknikutvecklingen.

En annan faktor som bidragit till att förstärka och snabba på utvecklingen är att många teknikområden relativt nyligen gått från att primärt vara forsknings- och utvecklingsområden till att nu användas i praktiken. Under de senaste åren har många verksamheter tagit steget från att bevaka teknikutvecklingen till att faktiskt börja använda den i praktiken. När tekniken går från teoretiska koncept till faktiska produkter och tjänster tas ytterligare steg i innovationsprocessen.[100] Därmed sker kommersialisering, anpassning, vidareutveckling och korsbefruktning med annan teknik i snabb takt.

Ett välkänt sätt att beskriva hastigheten i dagens teknikutveckling är den så kallade Moores lag, uppkallad efter en av företaget Intels grundare Gordon E. Moore. Förenklat kan Moores lag sammanfattas i att antalet transistorer i en integrerad krets fördubblas ungefär vartannat år, vilket också skett de senaste decennierna. Moores lag kan, utöver beräkningskraft, appliceras på allt från uppkopplingshastigheter, lagringsutrymme, kamerasensorer och annan teknik som är central inom digitalisering. Allt som har beräkningar som grund, och som digitaliseras, kan alltså utvecklas enligt denna exponentiella lag. Det här har skett inom en mängd områden, men vi är ännu bara i början.[101]

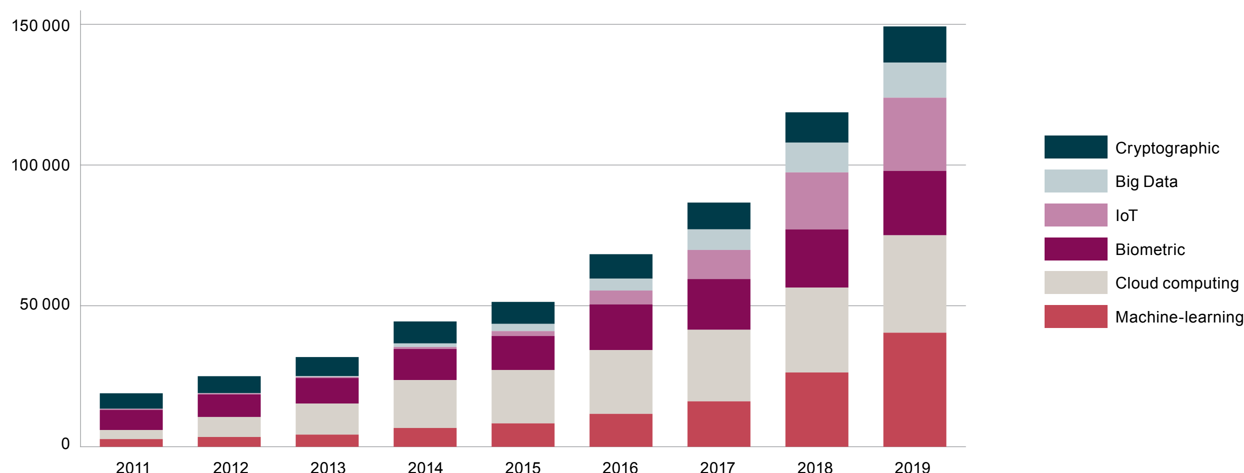
Exponentiellt tänkande är inte intuitivt. I en värld med exponentiell utveckling ökar därför diskrepansen mellan den värld vi lever i och vår förmåga att förstå och förutspå framtiden. Ett exempel kan tas i om vi tar 30 linjära steg jämfört med 30 exponentiella. 30 linjära steg tar oss ungefär 30 meter bort. 30 exponentiella steg tar oss däremot en miljard meter bort, eller motsvarande 26 varv runt jorden. Översatt till teknikutveckling kommer de kommande 100 åren, enligt denna exponentiella lag kallad *The Law of Accelerating Returns*, att motsvara 20 000 år av teknologisk utveckling.[102]

Ett annat sätt att illustrera hastighet och fokus i teknikutvecklingen är genom statistik över antalet patentansökningar. FN-organet World International Property Organization (WIPO) publicerar regelbundet global statistik över antalet patentansökningar.[103] En sökning i deras publika databas över globala patent avseende maskininlärning, molnlösningar, biometri, Internet of things (IoT) och big data illustrerar trenden tydligt. Enbart under perioden 2016 – 2019 har antalet publicerade patent fördubblats.

Diagrammet nedan visar tillväxten av antalet publicerade patent som innefattar nyckelorden machine-learning, cloud computing, biometric, IoT, big data och cryptographic mellan åren 2011 och 2019.

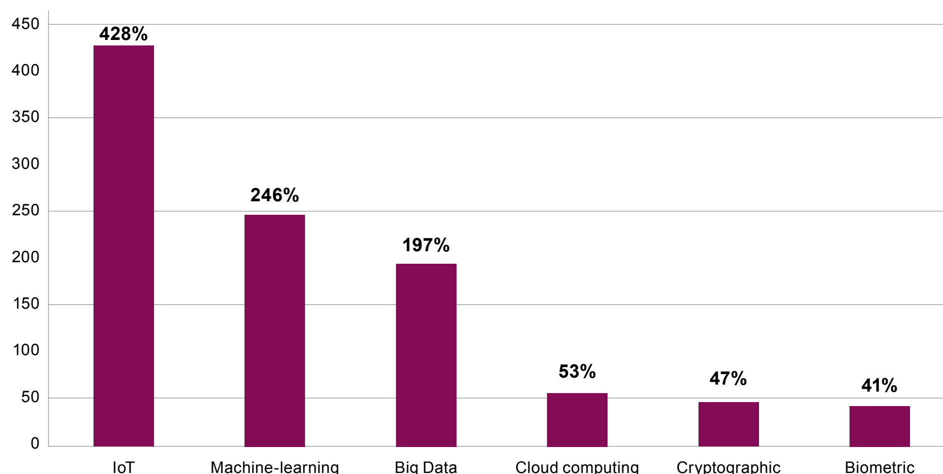
100. https://www.fincalabs.com/agile-innovation-framework-en/.
101. https://greentech.warpinstitute.se/exponentiella-lagar/.
102. https://greentech.warpinstitute.se/exponentiella-lagar/.
103. https://patentscope.wipo.int/search/en/search.jsf.

Antal publicerade patent som innehåller respektive sökterm, 2011-2019



En närmare fördjupning i statistiken visar att det är inom IoT som den största ökningen skett. Under år 2019 publicerades mer än fyra gånger så många patent som innehöll sökordet IoT under jämfört med år 2016. Diagrammet nedan visar den procentuella tillväxten av antalet publicerade patent per år i en jämförelse mellan åren 2016 och 2019. Tillväxten i antalet publiceringar var mer än 40 procent per år för samtliga söktermer.[104]

Tillväxt i antalet publicerade patent per år vid en jämförelse mellan åren 2016 och 2019



104. https://patentscope.wipo.int/search/en/search.jsf (sökningen genomfördes med inställningen ”Any Field”).

5.2 Personuppgifternas livscykel

Personuppgifter hanteras vanligen i en livscykel som börjar med att uppgifterna samlas in och avslutas med att de förstörs. Däremellan lagras, säkras, bearbetas och används samt transporteras uppgifterna – men inte nödvändigtvis i den ordningen. Redovisningen av utvecklingen på it-området delas här in utifrån livscykelns olika delar.

För att beskriva teknikutvecklingen har utgångspunkten tagits i vad som kan sägas vara personuppgifternas livscykel. Cykeln börjar med att uppgifterna samlas in/upprättas och avslutas med att uppgifterna förstörs eller arkiveras. Inom vissa verksamheter finns krav på att uppgifter ska sparas, antingen för viss tid eller för evigt. I sådana fall avslutas livscykeln med att uppgifterna arkiveras. Däremellan lagras, delas, bearbetas och används uppgifterna – men inte nödvändigtvis i den ordningen. Under hela livscykeln behöver också personuppgifterna säkras.

I den tidiga datoriserade bearbetningen av personuppgifter skedde behandlingen som regel i en bestämd och förutsägbar ordning. Efter den inledande insamlingen/upprättandet, följde lagring och säkring, bearbetning/användning, eventuell med en eller flera transporter och sist förstörande. Den tekniska utvecklingen har medfört att de olika stegen i livscykeln idag kan ha en annan, mer oförutsägbar ordningsföljd och ske i ett antal loopar.

Idag finns till exempel teknik där uppgifter säkras genom kryptering och bearbetas direkt i enheten som uppgifterna samlats in med – det vill säga innan uppgifterna lagras eller transporteras. Uppgifter kan också samlas in, bearbetas och förstöras i en och samma enhet och i realtid, utan att behöva transporteras. I andra fall sker transport av stora volymer personuppgifter kontinuerligt mellan samtliga steg i livscykeln – exempelvis när uppgifterna lagras och bearbetas i molntjänster som administreras av en tredje part.

Totalt beskrivs i det följande avsnittet sexton aktuella teknikutvecklingsområden, fördelade på de olika delarna i livscykeln. Vissa avsnitt innehåller mer djuplodande fördjupningar, medan andra avsnitt mer utgör allmänna beskrivningar av teknikområden som många gånger förutsätter insamling, bearbetning, transport, säkring, lagring och förstöring/arkivering av stora mängder data. Ofta dessutom personuppgifter.

5.3 Teknik för att samla in data

De omfattande affärsmöjligheter som ligger i stora datamängder har skapat starka incitament för att utveckla teknik för att samla in data.

Nya typer av *sensorer och sändare* utvecklas mot att bli allt mindre men samtidigt mer kraftfulla, vilket gjort det väsentligt lättare att samla in stora datamängder.

Ytterligare ett område där teknikutvecklingen gått snabbt framåt de senaste åren handlar om nya *former för interaktion mellan människa och dator.* På kort tid har röststyrningsteknik fått ett brett genomslag och spridits från mobiltelefoner och datorer till bland annat bilar, klockor, hörlurar och olika smarta prylar i hemmet som till exempel TV-apparater. Även teknik för avläsning av fingeravtryck och ansiktsigenkänning utvecklas snabbt.

Utvecklingen inom *Internet of things, IoT*, utgör ett särskilt riskområde. Den omfattande insamlingen av data som sker på nätet flyttar genom IoT ut i den fysiska världen. Kombinationen av utveckling inom ”smarta städer” och ”smarta hem” gör att vi omges av allt mer potentiellt integritetskränkande teknik – såväl i det offentliga rummet som i intima hemmiljöer. En stor andel IoT-enheter har visat sig ha bristande säkerhet. Forskare har till exempel visat hur man kan ta kontroll över en modern bil via ett trådlöst nät, eller via fjärrstyrning manipulera en pacemaker eller insulinpump.

Ytterligare ett riskområde är teknik för *webbskrapning* som automatiskt samlar in data från exempelvis sociala medier. Kännetecknande är ofta att informationsmängderna blir så stora att det blir oöverblickbart. Ett färskt exempel är ett företag som samlat in tre miljarder ansiktsbilder från miljoner olika webbplatser.

Risker för den enskilde individen med den ökande datainsamlingen handlar bland annat om att det blir allt svårare att upptäcka, kontrollera eller välja bort att data om vårt beteende och rörelsemönster samlas in – dels på nätet, dels i den fysiska världen.

En särskild typ av datainsamling som i ökande utsträckning används inom allt fler samhällsområden handlar om insamling av *biometriska uppgifter.* Biometri innebär att mäta kroppens egenskaper (till exempel hand- eller fingeravtryck, mönster i ögats iris, ansikts- eller kroppsform och röstavtryck) eller individers beteenden (till exempel gångstil, rörelse- och talmönster, handstil, ansiktsuttryck och sömnmönster) för att verifiera, autentisera eller identifiera individer. Användning av biometriska uppgifter kan skapa ökad bekvämlighet, snabbhet och säkerhet. Samtidigt medför den ökande användningen av biometriska uppgifter betydande integritetsrisker. En av de främsta riskerna handlar om att biometriska data (till skillnad från till exempel lösenord eller passerkort) inte kan bytas ut om uppgifterna skulle hamna i orätta händer. De biometriska uppgifterna är beständiga, vilket gör en integritetsförlust svår att reparera.

Personuppgifter har kommit att bli ett centralt värde i den digitala ekonomin och jämförs inte sällan med olja, guld eller ett slags valuta. Jämförelsen med olja bygger på att data är ett nödvändigt bränsle i så gott som alla branscher. Liksom olja behöver data också förädlas för att vara användbar.

I princip alla företag, myndigheter och organisationer behandlar idag personuppgifter på ett eller annat sätt. För en del företag utgör data själva grunden för affärsmodellen och i de allra flesta verksamheter finns också stora möjliga nyttor och vinster med att på olika sätt bearbeta, analysera och dela data.

Data är också själva grunden för tillväxt inom åtskilliga branscher och utgör därmed en renodlad handelsvara. Personuppgifter säljs som produkt och insamling av uppgifter erbjuds som tjänst. Att uppskatta omsättningen i den globala handeln med data är svårt, men som fingervisning kan nämnas att enbart intäkterna för datamäklarbranschen (eng. data brokers) år 2018 uppskattades till 21 miljarder amerikanska dollar.[105]

Datamäklare är företag som har som affärsidé att samla in personuppgifter och sälja dem vidare, ofta paketerade till exempel som konsumentprofiler. En konsumentprofil kan innehålla både demografiska och geografiska uppgifter, men också uppgifter om den enskildes livsstil och intressen. Personuppgifterna kan komma från vitt skilda källor: sociala medier, offentliga register eller andra företags kundregister. Sammantaget kan informationen användas till exempel för att anpassa marknadsföring, upptäcka bedrägerier eller göra risk- och kreditbedömningar. När den här typen av datapaketering köps som tjänst ingår ofta såväl insamling, rensning, löpande uppdatering och anpassning av data.

Möjligheterna att tjäna pengar på data utgör en stark drivkraft bakom utvecklingen av teknik för att samla in personuppgifter. En stor andel av uppgifterna samlas in med den enskilde individens medgivande exempelvis via sociala media, strömningstjänster, appar, digitala tjänster eller när vi handlar via nätet. För att kunna använda en digital tjänst ombeds vi bli medlemmar eller starta ett konto, där vi i användarvillkoren godkänner att uppgifter om oss samlas in. Samtidigt är komplexiteten stor i hur data delas mellan företag. Ofta är det för den enskilde individen oöverskådligt och svårt att bedöma vilka företag som kommer få tillgång till ens personuppgifter och varför. Hur handel med data i den digitala annonsindustrin går till beskrivs mer utförligt i avsnitt 5.4.3.

I flera av de intervjuer som IMY genomfört i arbetet med denna rapport framhålls den ökande insamlingen av data om vårt beteende och rörelsemönster, dels i den fysiska världen, dels på nätet, som den mest betydelsefulla teknikutvecklingen som påverkat den personliga integriteten under de senaste åren. Utvecklingen ger en mängd aktörer tillgång till en fullständig bild av våra liv, våra intressen, våra kontakter med mera. Det faktum att uppgifter delas mellan olika aktörer på ett sätt som ofta är svåröverblickbart för den enskilde individen gör integritetsriskerna större.

Företag driver på utvecklingen genom att kontinuerligt utveckla nya affärsmodeller som bygger på att erbjuda en digital tjänst mot att företaget får tillgång till – och därmed kan tjäna pengar på – data om användaren.

105. The Economist; *Are data more like oil or sunlight?*.

Konsumentverket lät 2017 göra en kartläggning av hur personuppgifter används som betalningsmedel. Problematiska beteenden som Konsumentverket identifierat handlar bland annat om *svepande datainsamling* som inte är transparent, det vill säga när mer data samlas in än vad som behövs för det uttalade syftet och *tredjepartsinsamling*, det vill säga när personuppgifter samlas in och hanteras av någon annan part än den som en konsument har en tydlig relation till. Även *spel riktade till barn*, med marknadsföring eller köpuppmaningar i spelen, och så kallad *clickbait-journalistik*, det vill säga webbinnehåll som syftar till att generera inkomster från online-annonsering med sensationella rubriker eller iögonfallande bilder som lockbete ses av Konsumentverket som problematiskt.[106]

Drivkraften att samla in och bearbeta personuppgifter kan vara så stark att verksamheter väljer att göra det utan att enskilda individer är medvetna om insamlingen, samtycker till den eller samtycker till hela tjänstens omfattning.[107] Detta strider mot dataskyddsförordningens grundläggande principer och krav på rättslig grund för behandlingen, men riskerar i hög utsträckning att förbli ouppträckt.

Möjligheten att tjäna pengar på personuppgifter gör det också till en attraktiv tillgång för olika typer av hotaktörer. På Darknet – den hemliga, dolda delen av internet där en hel del olaglig verksamhet pågår – går det att beställa olaglig insamling av personuppgifter som tjänst. I rapporten ”In the dark” beskrevs hur stulna och känsliga personuppgifter säljs via olika handelsplatser på Darknet.[108] Prislistor figurerar med information om hur mycket det kostar att komma över en individs inloggningsuppgifter till olika bank- och betalningstjänster, sociala media-lösenord etcetera. Det går också att beställa attacker mot ett företag eller en organisation som hanterar stora mängder känsliga personuppgifter. I rapporten ges också exempel på försäljning av stora datafiler från tidigare genomförda dataintrång riktade mot specifika webbplatser. Som ett exempel kan nämnas att det enligt rapporten kostar 3 200 amerikanska dollar att få tillgång till 65 miljoner dataposter från en av de marknadsledande släktforskningstjänsterna.

106. Konsumentverket rapport 2017:4; *Personuppgifter som betalningsmedel*.

107. Detta förutsätter att den rättsliga grunden är samtycke.

108. https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

Det finns också flera exempel på hur företag och myndigheter har utsatts för utpressningsförsök när bedragare på något sätt har kommit åt inloggningsuppgifter i en verksamhet eller på annat sätt fått tillgång till omfattande datasamlingar. Ett exempel är den omfattande läckan av privata patientjournaler från finska psykoterapibolaget Vastaamo som har beskrivits som en omfattande och sällsynt hackerattack. Journalerna innehåller intima uppgifter om patienternas privatliv men även deras adresser och fullständiga namn. Patienter vars journaler läckt har utpressats att betala pengar för att stoppa spridningen av de privata uppgifterna på nätet. Ett antal journaler ska ha lagts ut på darknet.[109]

Sammanfattningsvis kan konstateras att incitamenten för att utveckla teknik för att samla in data är stora, givet de omfattande affärsmöjligheter som ligger i värdet av data. Nedan ges fördjupningar inom några teknikutvecklingsområden som särskilt ökat möjligheterna att samla in data.

5.3.1 Sensorer och sändare

En förutsättning som gjort det betydligt lättare att samla in mer data är utvecklingen av nya typer av sensorer och sändare. Tack vare sensorer och sändare som tar mindre utrymme, men samtidigt är mer kraftfulla, har nya och förbättrade möjligheter skapats att samla in data i alla slags former: bild, ljud, rörelse, temperatur, tryck, ljus, position, lutning, magnetism etcetera. Data kan samlas in i allt större volymer, i nya format, på nya platser och i nya sammanhang.

Nätverk av sensorer kan tillsammans samla in data över ett mycket stort fysiskt område. De kan monteras fast – på till exempel en byggnad – men också kopplas till rörliga objekt som fordon eller drönare. Vissa typer av sensorer kan också följa med i naturens rörelser, till exempel flyta med i vattendrag. Eftersom sensorer och sändare beräknas kunna krympas till samma storlek som ett dammkorn beskrivs teknikutvecklingen ibland som ”smart damm”.[110]

Exempel på användningsområden för sådana mikroskopiska sändare finns till exempel inom försvarsindustrin, meteorologiska mätningar, kontroll av miljöföroreningar och skogsbränder samt bevakning av produktionsprocesser och anläggningar.[111] Potentialen i utvecklingen har – på gott och ont – beskrivits som att multiplicera Internet of Things miljoner gånger.[112] Konkreta integritetsrisker som följer av denna typ av sensorer och sändare handlar om att enskilda individer ofrånkomligen riskerar att fångas upp, även om det inte är syftet med datainsamlingen. Under vissa omständigheter kan det vara enkelt att identifiera enskilda individer, i synnerhet om datan samkörs med andra typer av uppgifter.

En typ av sensorer och sändare som har blivit allt vanligare i takt med att tekniken och funktionaliteten utvecklats, är kroppsnära teknik, så kallade ”wearables”, som kan mäta kroppens signaler och skicka feedback till användaren. Träningsarmband, pulsklockor och smarta klockor är några exempel på sådan kroppsnära teknik. En rad uppgifter om den enskildes hälsa och aktiviteter samlas in och individen får löpande återkoppling på dessa faktorer. Särskilt användbar blir utrustningen om den kopplas ihop med andra data från individen. En rad exempel på hur kroppsnära teknik kan skapa stor nytta finns inom sjukvården. Med hjälp av biosensorer kan olika värden hos patienten följas upp på ett helt nytt sätt. Kopplas tekniken till nätverk av kommunicerande enheter med inomhuspositionering på sjukhusens personal och utrustning kan också sjukhusens logistik effektiviseras.

Olika typer av sensorer och sändare används för att följa till exempel rörelsemönster eller beteenden hos enskilda individer. De kan användas för uppföljning med återkoppling till den enskilde, för riktad marknadsföring av olika varor eller tjänster, eller också i kontrollsyfte. Ett exempel är uppkopplade sensorer i försäkringstagares fordon, som samlar in detaljerad data om förarens körmönster med mera, som bearbetas av försäkringsbolagen och används för bland annat dynamisk prissättning av försäkringarna i realtid.[113] Ett annat exempel är nya biosensorer som kan mäta organiska material och bakterier med hög precision[114] och kan användas inom bioteknikområdet.

109. https://www.svt.se/nyheter/utrikes/tusentals-journaler-lack-ta-fran-finskt-terapiforetag.

110. https://www.forbes.com/sites/bernardmarr/2018/09/16/smart-dust-is-coming-are-you-ready/?sh=f729bcd5e41a.

111. International Working Group on Data Protection in Technology: *Working Paper on Sensor Networks (Smart Dust)*.

112. https://www.forbes.com/sites/bernardmarr/2018/09/16/smart-dust-is-coming-are-you-ready/?sh=f729bcd5e41a.

113. https://www.pwc.co.uk/issues/data-protection/insights/the-internet-of-things-is-it-just-about-gdpr.html.

114. https://www.startus-insights.com/innovators-guide/biotech-innovation-map-reveals-emerging-technologies-startups/.

En typ av sensorer och sändare som är extra intressant ur integritetssynpunkt är teknik med koppling till geospatial teknologi. Området omfattar bland annat geografiska informationssystem, geografiska positioneringssystem (exempelvis GPS), informationsinsamling om jorden via satelliter och höghöjdsflygplan samt navigering. Dessa sensorer och sändare kan bland annat användas för att samla in data om var en person befinner sig och hur enskilda individer rör sig.[115]

Som bland annat tidningen New York Times visat i flera större artiklar utgörs en stor integritetsrisk av att det även i ”anonyma” dataset, som innehåller många poster och positioneringsdata, ofta är enkelt att identifiera enskilda individer. Utifrån ett dataset med 50 miljarder poster positionsdata om 12 miljoner människor som samlats in i appar lyckades New York Times enkelt identifiera ett antal enskilda individer till exempel genom hur en viss telefon återkommande rörde sig mellan en viss adress på dagtid (en arbetsplats) och en annan på kvällstid (hemmet). Med några enkla kompletterande sökningar i öppna källor gick det lätt att identifiera enskilda. När en viss telefon väl har kopplats till en enskild individ är det i nästa steg möjligt att få en komplett bild av personens rörelsemönster med allt ifrån läkar- eller kyrkobesök till besök hos vänner och familj.[116]

En särskild typ av datainsamling med geografisk positionering som aktualiserats under 2020 är olika typer av appar som utvecklats för att spåra kontakter och smittvägar med anledning av coronapandemin. Såväl Google och Apple som statliga myndigheter i flera länder har utvecklat och implementerat olika applikationer för smittspårning. Tjänsterna bygger på de sensorer och sändare som finns inbyggda i användarnas smarta telefoner – exempelvis bluetooth och GPS. I dess enklaste form meddelar appen användaren om denne potentiellt exponerats för coronavirussmitta, men apparna kan också användas av myndigheter för att spåra hur viruset sprider sig och för att övervaka var potentiellt smittade personer befinner sig. I vissa länder är användandet av appen frivilligt och i andra är det obligatoriskt. Några är transparenta i hur insamlade personuppgifter behandlas och andra inte.[117] En del är designade med en decentraliserad modell där data om användarna stannar på användarnas mobiler, medan andra skickar alla data till en central server.[118]

Den här typen av appar medför en rad integritetsutmaningar, kopplade till hur de utformas och används. De kan innefatta både geografisk spårning och i vissa fall även ansiktsigenkänning, vilket utgör ett särskilt riskområde. I den utsträckning apparna har utvecklats snabbt, utan att personuppgifts- och integritetsskyddsperspektivet fullt ut har beaktats, och utan att de långsiktiga effekterna och konsekvenserna av dem har analyserats, kommer det ha stor betydelse hur apparna monteras ner på ett ansvarsfullt sätt, när pandemin är under kontroll.

Även under andra omständigheter än en världsomspännande pandemi ger utvecklingen och användningen av nya sensorer och sändare upphov till en rad integritetsrisker. Oproportionerligt omfattande datainsamling och att datan används för andra ändamål än de ursprungligen samlats in för är några exempel. Frågor som aktualiseras rör till exempel hur information ska ges till enskilda när verksamheter har många sensorer utspridda över stora geografiska områden, hur – om samtycke används som rättslig grund – samtycke ska kunna samlas in innan sensorer samlar in data och hur sensorerna ska kunna exkludera individer som inte gett sitt samtycke.[119]

För den enskilde individen handlar integritetsriskerna kopplat till nya typer av sensorer och sändare bland annat om att det blir allt svårare att överblicka vem som har vilken information om individen och för vilka syften. Teknik som utvecklas för att öka tryggheten kan, i fel händer, enkelt vändas till ett säkerhetshot. GPS-sändare med larm används bland annat i äldreomsorgen och upplevs av många anhöriga öka tryggheten. I fel händer kan de utnyttjas för att identifiera äldre som är tacksamma offer för bedrägerier eller annan brottslighet. Ett annat exempel på användningsområde är när föräldrar använder GPS-teknik för spårning av barns och ungas mobiler – oftast i trygghetsskapande syfte. Samma teknik kan dock användas för en illegitim kontroll och övervakning av barn och ungdomar. Kvinnojourer i Sverige har också rapporterat om ett växande problem i att män övervakar kvinnor genom GPS-spårning via till exempel appar i mobiltelefonerna för att kunna kontrollera var kvinnan befinner sig.[120]

115. https://www.geospatialworld.net/article/geospatial-industry-trends-2020-be-disruptive-or-be-irrelevant/.

116. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

117. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

118. https://computersweden.idg.se/2.2683/1.733648/frankrike-bluetooth-corona.

119. Även vid andra rättsliga grunder är det viktigt att veta hur information om insamlingen kan ges, så att den blir transparent för den registrerade.

120. https://sverigesradio.se/sida/artikel.aspx?programid=160&artikel=7090304.

Sammanfattningsvis erbjuder nya typer av sensorer och sändare stora möjligheter, men innebär samtidigt integritetsrisker som behöver adresseras och tas på allvar. Det är i praktiken inte möjligt för den enskilde individen att överblicka all datainsamling som sker via sensorer och sändare. Det är därför viktigt att verksamheter som samlar in information tar det ansvar som följer av dataskyddsreglerna så att insamlingen görs transparent för den enskilde. Ett underminerat integritetsskydd riskerar att helt undergräva medborgarnas rätt till privatliv om teknikutvecklingen tar sin utgångspunkt i redan bristfälliga modeller, där integritetsskyddsaspekterna inte utvecklas i samma takt som tekniken. Betydelsen av att perspektiven går hand i hand accentueras ytterligare mot bakgrund av den exponentiella utvecklingstakten i digitaliseringen.

5.3.2 Teknik för interaktion mellan människa och dator

Ett annat område där teknikutvecklingen gått snabbt framåt de senaste åren handlar om nya former för interaktion mellan människa och dator. Utvecklingsområdet omfattar planering, design och studier av interaktiva produkter och tjänster. Det är ett tvärvetenskapligt ämne som knyter samman exempelvis datavetenskap och informatik med flera andra forskningsområden som till exempel kognitionsvetenskap. Inom detta område pågår en snabb teknisk utveckling som förändrar förutsättningarna för hur vi interagerar med datorer och vilken information om oss och vår omgivning som samlas in och bearbetas.

Från de första datorernas hålkort, via tangentbord, grafiska operativsystem, pekdon och tryckkänsliga skärmar – bygger dagens teknik ofta på röststyrning eller avläsning av fingeravtryck och ansiktsigenkänning.

Allt fler användare nyttjar möjligheten att kommunicera med till exempel sin mobiltelefon, en TV eller en smart högtalare i hemmet via kommandon eller frågor till en digital assistent. Även om de digitala assistenterna lanserades redan i början av 2010-talet har antalet användare som nyttjar röststyrning ökat kraftigt de senaste åren. En bidragande förklaring till detta är att tekniken, genom att den blivit mindre och kopplats mot molnlösningar, nu kan nyttjas i en rad andra befintliga produkter med bred spridning.[121]

De digitala assistenterna har också blivit smartare med åren. För svenska användares del har tekniken blivit mer relevant i takt med att flera av de digitala assistenterna under de senaste åren lanserats på svenska. År 2019 uppgav 1 av 20 svenskar att de har en uppkopplad högtalare hemma, till exempel Google Home eller Amazon Echo.[122]

Från att röststyrning introducerats på marknaden i mobiltelefoner, på webbplatser och i datorer, är det idag vanligt att tekniken finns i bilar, klockor, hörlurar och olika smarta prylar i hemmet som till exempel TV-apparater. Ett annat konkret exempel på en ny form av interaktion mellan användare och teknik som på kort tid slagit igenom på bred front är ansiktsigenkänningsteknik för att låsa upp mobiltelefoner.

Teknik som bygger på igenkänning av en specifik individ – till exempel en digital assistent som känner igen och enbart lyder kommandon från en viss röst, eller en mobiltelefon som låses upp genom avläsning av ägarens fingeravtryck – innebär att biometriska uppgifter hanteras. För den enskilde individen finns här inneboende risker som handlar till exempel om att inspelade frågor eller kommandon i fel händer kan manipuleras eller användas för andra syften, till exempel stölder, intrång eller bedrägerier.

Även när kommunikationen mellan människa och teknik inte handlar om att identifiera en specifik individ finns konkreta integritetsrisker. De stora tech-bolagen Google, Amazon, Facebook, Apple och Microsoft har alla fått kritik för att ha gett underleverantörer tillgång till användares röstinspelningar för bearbetning i syfte att förbättra assistenternas talanalys. För att digitala assistenter ska kunna svara på annat än väldigt enkla frågor krävs omfattande beräkningskraft, vilket innebär att frågor och kommandon behöver överföras till leverantörens centrala servrar och analyseras där. Tekniken kan bara utvecklas kontinuerligt med hjälp av feedback – vilket ges dels från användare, dels genom att teknikföretagets anställda kontinuerligt lyssnar på och kontrollerar ett stort antal ljudinspelningar.

121. International Working Group on Data Protection in Telecommunications; *Working paper on data protection risks of voice-controlled devices*, 2020.

122. Internetstiftelsen Svenskarna och Internet 2019.

Forskning har visat att Apples Siri, Amazons Alexa och Google Assistant aktiveras av misstag upp till 19 gånger per dag.[123] Ett uppmärksammat exempel på hur Siri aktiverats av misstag gavs när den brittiska försvarsministern 2018 under ett tal i brittiska underhuset ljudligt avbröts av sin digitala assistent – någon del av hans anförande om säkerhetsläget i Syrien hade råkat aktivera assistenten. Även under direktsända presskonferenser i Vita huset eller nyhets- och sportsändningar har det hänt att Siri plötsligt inflikat en kommentar eller fråga.[124] Att det är vanligt att talassistenter aktiveras av misstag har också bekräftats av visselblåsare från de stora tech-företagen. I praktiken innebär detta att anställda hos underleverantörer regelbundet kunnat avlyssna situationer som de inblandade högst sannolikt inte velat dela med sig av – affärsmöten, läkarbesök, droguppgörelser och sexuella möten för att ge några exempel.[125]

Gränssnittet mellan människan och datorer handlar dock inte bara om röststyrning. Tekniken kompletteras nu allt oftare med rörelsesensorer och kameror som kan identifiera och tolka gester. Användaren slipper därmed gå fram till den tekniska enheten för att till exempel trycka på en start-knapp – det kan räcka med att göra en viss gest. Samtidigt som bekvämligheten ökar, ökar även risken för att tekniken aktiveras av misstag. Det blir också allt svårare för enskilda individer att välja bort att fångas upp av teknik som installerats av andra, till exempel röststyrd teknik som finns i vänners hem.

5.3.3 Internet of Things

Som beskrevs i avsnitt 5.1 är Internet of Things, IoT, ett av de teknikområden där antalet beviljade patent ökat allra mest under de senaste åren. Området innefattar olika apparater, maskiner, mätutrustning och fordon som har inbyggd teknik och internetuppkoppling, men typiskt sett inte ses som datorer.[126]

Begreppet IoT används vanligtvis för att beskriva ett nätverk av smarta enheter som känner av eller interagerar med omgivningen. Enheterna i nätverket kan kontinuerligt samla in information, reagera på den och kommunicera både med människor och med andra enheter. IoT kan vara vardagsföremål som vitvaror, termostater, belysning, TV-apparater, elektroniska lås och larm, kläder eller bilar, men också utrustning i industri, infrastruktur eller vården. Utvecklingen går mot att IoT används inom allt fler samhällsområden och på allt fler geografiska platser för att samla in data. Sverige har ett strategiskt innovationsprogram inriktat mot IoT, som finansieras av Vinnova, Energimyndigheten och Formas samt externa aktörer. Programmet ger stöd till innovativa projekt, inriktade på sakernas internet, som genomförs över hela landet.[127]

När det handlar om utrustning som vanligen finns i hemmet används ibland begreppet ”det smarta hemmet” eller ”det uppkopplade hemmet”. Antalet uppkopplade saker i de svenska hemmen har ökat de senaste åren. I undersökningen Svenskarna och Internet 2019 uppgav 54 procent av den svenska befolkningen över 16 år att de har en uppkopplad enhet hemma, mobiltelefoner och datorer exkluderat. Det var en ökning från 2018 (vilket var första året frågan ställdes i undersökningen) då siffran var 50 procent. De flesta uppger dock att de bara har några enstaka uppkopplade saker. För 39 procent rör det sig om 1–5 uppkopplade saker, medan 9 procent uppgav att de har 6–10 saker. Det finns en okunskap kring om man har några uppkopplade saker hemma och sannolikt kring vad begreppet ”uppkopplad sak” innebär, för liksom 2018 anger 7 procent att de inte vet om de har någon uppkopplad sak i sitt hushåll.[128]

Även inom ramen för ”smarta städer” blir uppkopplade apparater och sensorer i det offentliga rummet allt vanligare. De bakomliggande syftena med att samla in data kan exempelvis vara att effektivisera och automatisera olika typer av kontroller och mätningar. Exempel på användningsområden finns till exempel i transportsektorn, där det kan handla om att koppla ihop fordon med smarta telefoner, andra fordon och IoT-sensorer i väg- och järnvägsnätet eller i kollektivtrafiken för ökad trafiksäkerhet, fordonsdiagnostik med mera.[129] På fastigheter kan sensorer till exempel samla in data för effektivare hantering av säkerhet, ljus och diagnostik[130] Uppkopplade enheter kan också finnas till exempel i mätutrustning och ställdon i smarta elnät och transport- och vattensystem. Genom att enheterna är anslutna till internet kan de fjärrstyras av människor eller av andra maskiner. De kan också skicka data som används för mätningar, diagnos och automatisk styrning.[131]

123. https://www.forbes.com/sites/kateoflahertyuk/2020/02/26/new-amazon-apple-google-eavesdropping-threat-should-you-quit-your-smart-speaker/.

124. https://www.theguardian.com/commentisfree/2019/jul/30/apple-siri-voice-assistants-privacy.

125. https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings.

126. Tekniken i IoT utgörs ofta av sensorer och sändare. Under rubriken Internet of things ligger här fokus på hur tekniken används, till exempel i smarta städer och uppkopplade hem.

127. Komet kommenterar 2020:27 *Sakernas internet – korta faktablad om aktuell teknik*.

128. Internetstiftelsen *Svenskarna och Internet 2019*. 2020 års rapport var primärt inriktad på effekter av coronapandemin och uppgifterna om uppkopplade saker, IoT, omfattades inte av 2020 års mätning.

129. https://www.startus-insights.com/innovators-guide/automotive-innovation-map-reveals-emerging-technologies-startups/.

130. https://www.iotsworldcongress.com/iot-smart-buildings-becoming-part-of-the-smart-grid/.

131. https://it-ord.idg.se/ord/sakernas-internet/.

I handeln kan insamling av data med IoT-enheter användas för att skapa bättre beslutsstöd kring kundupplevelser, lagerhållning, produktplacering, logistik med mera. Uppkopplade sensorer, så kallade beacons, i till exempel butiker och köpcentrum kan också användas för att erbjuda kunderna anpassade erbjudanden utifrån hur de rör sig i lokalerna. IoT kan också användas inom tillverkande industri genom insamling och bearbetning av data kring tillverkning, leverans, underhåll och lagerhantering genom smarta sensorer i syfte att optimera processerna och produktionen, samt för att ge direkt överblick över ett produktionssystem i realtid.[132]

Även offentlig sektor kan ha omfattande nytta av IoT i publika miljöer. Möjliga användningsområden kan vara smarta övervakningskameror för att öka trygghet och förebygga brott, uppkopplade enheter som bidrar till en effektiv hantering av vattenförsörjning, kollektivtrafik eller parkeringskontroll eller IoT för att förebygga eller upptäcka miljöutsläpp eller naturkatastrofer.[133] Sveriges kommuner och regioner, SKR, menar att IoT kan skapa nya möjligheter för välfärd och samhällsbyggnad. SKR har beskrivit hur tekniken kan komma till användning inom hälso- och sjukvård, fastigheter samt miljö och stadsutveckling. Samtidigt lyfter SKR frågor om säkerhet och integritet. SKR ser också behov av att klargöra gränssnitt och standarder och menar att kommuner och regioner som köper produkter kan påverka detta genom att vara tydliga med vilka krav de ställer när de gör upphandlingar.[134]

Flera av de experter IMY intervjuat i arbetet med denna rapport framhåller IoT som ett av de utvecklingsområden som haft störst påverkan på den personliga integriteten under de senaste tre åren. Kombinationen av utveckling inom ”smarta städer” och ”smarta hem” gör att vi omges av allt mer potentiellt integritetskränkande teknik – såväl i det offentliga rummet som i våra hem.

Ett sätt att uttrycka det är att den omfattande insamling av data som sker på nätet – som de flesta människor i åtminstone någon mån känner till – nu flyttar ut i den fysiska världen där den blir betydligt svårare att upptäcka, kontrollera och avskärma sig från.

I det ”smarta hemmet” sker insamling av data i en påfallande intim miljö, med ljudinspelning av barn och andra som inte väljer själva. Uppkopplade saker som ringklockor, lås, larm, kameror eller högtalare kan samla in persondata också om andra än ägaren. Detta innebär att möjligheten för enskilda personer att välja bort potentiellt integritetskränkande teknik redan har och fortsätter att drastiskt försämras. Det är också svårt för enskilda individer att flytta och ”byta plats” om de till exempel skulle vara missnöjda med personuppgiftsbehandlingen i en smart stad. I takt med att den här utvecklingen sker blir det allt svårare att hitta privata utrymmen för enskilda.

Internetstiftelsen lyfter i sin guide om IoT flera integritetsrisker, bland annat att såväl privata som offentliga aktörer kan ha starka intressen att både öka datainsamlingen och använda insamlad data för andra ändamål än vad de ursprungligen samlats in för. Att sälja data om användarna är en del av intäktsplanen för många IoT-företag.[135]

Säkerhetsutmaningarna kopplade till IoT kan röra sig om angrepp mot enskild utrustning med omfattande negativa konsekvenser, både för enskilda individer och verksamheter. Forskare har till exempel visat hur man kan ta kontroll över en modern bil via ett trådlöst nät, eller via fjärrstyrning manipulera en pacemaker eller insulinpump.[136]

En mer vardagsnära integritetsrisk handlar om att de flesta medborgare sannolikt har otillräckliga kunskaper när det gäller att tömma uppkopplade saker på information vid en eventuell andrahandsförsäljning, vilket kan resultera i att stora mängder personliga data oavsiktligt hamnar i den nya ägarens händer.

Riktas angrepp mot uppkopplade saker inom industrin kan angripare få kontroll över samhällskritiska processer inom exempelvis värme, vatten, el, transport eller finansiella tjänster. Försvarets forskningsinstitut (FOI) har i en rapport om risker relaterade till IoT beskrivit att ett av problemen är den stora mängden produkter med bristande säkerhet. Många av dessa produkter har standardlösenord som är lätta att komma över. Ofta är de inte designade med hänsyn till säkerhet alls och det fysiska skyddet är i allmänhet svagt.[137] En systemägare kanske inte ens känner till att de har utrustning som är nåbar via internet. Ett exempel på hur IoT med bristande säkerhet kan utnyttjas är ett it-säkerhetsföretag, som vid ett test lyckades komma över omfattande datamängder från ett amerikanskt casino. Angreppet skedde via ett i casinot nyinstallerat akvarium, där vattnets temperatur och salthalt kontinuerligt kontrollerades och kunde fjärrstyras.[138]

132. https://www.startus-insights.com/innovators-guide/manufacturing-innovation-map-reveals-emerging-technologies-startups/.

133. https://www.allerin.com/blog/4-ways-the-government-sector-can-benefit-from-iot.

134. Komet kommenterar 2020:27 *Sakernas internet – korta faktablad om aktuell teknik*.

135. Internetstiftelsen; *Internetguide #43 Internet of things – En guide till sakernas internet*.

136. The Economist; *A connected world will be a playground for hackers*.

137. Totalförsvarets forskningsinstitut (FOI) *NCS3 Studie - IoT-relaterade risker och strategier*.

138. The Economist *A connected world will be a playground for hackers*.

5.3.4 Webbskrapning

Ytterligare ett teknikutvecklingsområde som ökat möjligheterna att samla in stora mängder är webbskrapningsprogram. Med hjälp av speciella program kan stora mängder data samlas in automatiskt, från exempelvis webbsidor och sociala media.[139] Exempel på webbskrapning är de tjänster som gör automatiska prisjämförelser mellan olika företag på internet. Tekniken benämns ”skrapning” eftersom programmen hämtar information från webbsidor, inte från de bakomliggande databaserna. Programmen påminner om den indexering sökmotorer gör när de samlar in innehållet på webbsidor, med den skillnaden att webbskrapningsprogrammen inte samlar in all information utan letar efter särskilda typer av information.

Datan kan sedan bearbetas på sätt som de enskilda individerna varken godkänt eller är medvetna om. Kännetecknande är ofta att informationsmängderna blir så stora att det blir oöverblickbart. Det finns idag företag som utvecklar och erbjuder webbskrapningstjänster. Ett exempel är ett internationellt företag som, för att möta behoven hos sina närmare 2 000 företagskunder, använder de sig av teknik som varje månad söker igenom åtta miljarder webbsidor.[140]

Med de mängder personuppgifter som finns tillgängliga på sociala medier är det lätt att se lockelsen för aktörer som av olika skäl vill kartlägga stora mängder individer. Facebook tillåter formellt inte att deras plattform webbskrapas. Samtidigt är angrepp förhållandevis enkla att genomföra och svåra att upptäcka. Hösten 2018 offentliggjorde Facebook att de raderat närmare ett sjuttiotal konton, appar och sidor som tillhörde två ryska företag som utvecklar ansiktsigenkänningsteknik för den ryska regeringen. Enligt Facebook hade företagen genom webbskrapning samlat in foton från andra användares konton i syfte att identifiera dem.[141]

Clearview AI är ett exempel på en tjänst som baseras på personuppgifter som samlats in med webbskrapningsteknik.[142] Webbtjänsten uppger att de samlat tre miljarder ansiktsbilder från Facebook, YouTube och miljoner andra webbplatser. Tjänsten, som sålts bland annat till rättsvårdande myndigheter i USA, gör det möjligt att med hjälp av ansiktsigenkänningsteknik matcha bilder av okända personer mot den gigantiska databasen.[143] Sökträffarna berättar i många fall både vem personen är, men ger också en förhållandevis heltäckande bild av till exempel personens aktivitet på sociala medier.

139. http://whitepapers.virtualprivatelibrary.net/Web%20Data%20Extractors.pdf.

140. www.scrapinghub.com.

141. The New York Times; *Facebook Says Russian Firms ‘Scraped’ Data, Some For Facial Recognition*.

142. https://www.svt.se/nyheter/inrikes/detta-ar-clearview-ai och New York Times *The Secretive Company That Might End Privacy as We Know It*.

143. IMY inledde under 2020 ett tillsynsärende där eventuell användning av Clearview AI inom svensk brottsbekämpning utreds.

Amerikanska poliser uppger att de med hjälp av söktjänsten kunnat lösa ett antal brott, allt från bedrägerier till barnpornografibrott och mord. Samtidigt väcker tjänster som Clearview AI omfattande frågor ur ett integritetsskyddsperspektiv. Tekniken gör det enkelt att söka rätt på enskilda individer – oavsett syfte – och belyser den ständigt närvarande risken för ändamålsglidning. Även om tjänsten har utvecklats för brottsbekämpande myndigheter och säkerhetsföretag har det framkommit hur tjänsten också använts som ett verktyg av vissa privatpersoner för att göra egna bakgrundskontroller av nya bekantskaper. Sofistikerad säkerhetsteknik blir, även om den ursprungligen utvecklats för offentliga eller kommersiella syften, snabbt attraktiv även för privatpersoner. Bredare spridning av ett sådant verktyg skulle i grunden förändra förutsättningarna för allt mänskligt samspel – både för behjärtansvärda syften, men också mer illasinnade. Möjligheten att, öppet eller i smyg, kunna ta ett foto av en person på gatan och på några sekunder få tillgång till både personens identitet och utförlig information om personen skulle på ett genomgripande sätt kunna förändra den personliga integritetens förutsättningar. Talande är att när tidningen New York Times, som var först med att skriva om Clearview AI, släppte nyheten om den kontroversiella appen var det med rubriken ”Slutet för den personliga integriteten?”.[144]

5.3.5 Insamling av biometriska uppgifter

En särskild typ av datainsamling som utvecklats snabbt de senaste åren handlar om insamling av biometriska uppgifter. Biometri innebär att mäta kroppens egenskaper eller individers beteenden, och på så vis hitta särskiljande egenskaper hos olika individer. Biometriska personuppgifter berättar vilka vi är, och de kan inte enkelt ändras och inte heller ersättas om de går förlorade. De är därför användbara för att identifiera unika identiteter, men innebär samtidigt särskilda risker ur ett integritetsperspektiv.

Att mäta kroppens egenskaper eller individers beteenden för att hitta särskiljande egenskaper hos olika personer är inte ett nytt fenomen. Fingeravtryck har använts inom polis- och rättsväsendet i syfte att identifiera brottslingar i mer än hundra år och redan på 1800-talet kunde signalister identifieras utifrån mönster i hur de signalerade punkter och bindestreck i morsekod.[145] Men området har utvecklats till att innefatta många andra tekniker, användningsområden och biometriska egenskaper, som kan samlas in både i fysisk kontakt med individen och på distans.

144. New York Times; *The Secretive Company That Might End Privacy as We Know It*.

145. https://www.gemalto.com/govt/inspired/biometrics.

Biometriska uppgifter är extra känsliga personuppgifter eftersom de i grunden beskriver vem individen *är*. Uppgifterna rör en persons ”fysiska, fysiologiska eller beteendemässiga egenskaper” och gör det möjligt att identifiera människor. De två huvudsakliga användningsområdena för biometriska uppgifter är att verifiera eller autentisera (till exempel att kontrollera att en individ verkligen är den som individen utger sig för att vara) och att identifiera en enskild individ. Biometri används inom många samhällsområden och i olika syften, som exempelvis bevakning och övervakning, släktforskning, inloggning i mobila enheter och personlig anpassning av tjänster och produkter.

Den ökade insamlingen och användningen av biometriska uppgifter har i stor utsträckning möjliggjorts och påskyndats av utvecklingen inom en rad andra teknikutvecklingsområden:

- **Sensorer och sändare** – gör det möjligt att samla in data som kan omvandlas till biometriska uppgifter, på fler platser, både vid direktkontakt och på distans.
- **Människa-datorinteraktion** – bygger på användningen av röst, personliga uttryck och beteendemönster för att interagera med datorerna och är därmed närbesläktat med beteendebaserad biometri
- **IoT** – innefattar bland annat kameror och annan uppkopplad utrustning som kan användas för att samla in och bearbeta biometrisk data
- **AI och big data** – har stor inverkan på beteendebaserad biometri eftersom de möjliggör avancerad bearbetning av ett mycket stort antal parametrar, samtidigt och i realtid[146]
- **Molnifiering av lagring** – möjliggör platsoberoende lagring och åtkomst av stora databaser med biometriska mallar.

Användning av biometriska uppgifter ställer därför extra stora krav på den som behandlar uppgifterna.

5.3.5.1 Olika typer av biometriska uppgifter

Traditionellt har biometri handlat om att samla in och analysera *fysiska egenskaper*. Det kan exempelvis handla om hand- eller fingeravtryck, DNA, mönster i ögats iris, öronform, ansikts- eller kroppsform och röstavtryck. Denna typ av biometri är mycket vanlig idag och används bland annat för att låsa upp smarttelefoner, till accesskontroll i byggnader och för registrering vid gränskontroller.

Trenden går mot att i allt större utsträckning även använda individens *beteende* för biometriska analyser. AI och annan teknisk utveckling har gjort det möjligt att använda uppgifter som tidigare ansågs oanvändbara – och kanske inte ens betraktades som personuppgifter – till att identifiera individer med stor säkerhet. Denna form av biometri används bland annat för att upptäcka avvikande mönster hos bankkunder (i syfte att förebygga bedrägerier) och för att identifiera och övervaka grupper och individer.

Exempel på beteendebaserad biometri är gångstil, rörelse- och talmönster, handstil, ansiktsuttryck och sömnmönster. Det kan också handla om mönster i hur användaren svarar på olika stimuli i en app, använder mobilen, skrollar i och skiftar mellan dialogfönster på webben eller använder tangentbordet.

De senaste åren har teknikutvecklingen inneburit att det kontinuerligt tillförs nya biometriska egenskaper, med unika styrkor och svagheter. Några aktuella exempel på biometriska egenskaper som det utvecklas ny teknik för är hjärnans signaler (EEG), hjärtrytm (ECG), doftprofil, venernas struktur under huden, läppar och dess rörelsemönster, svett, blod och öronens utseende.[147]

Varje biometrisk egenskap har sina för- och nackdelar vad gäller möjligheten att identifiera och särskilja individer. Det kan handla till exempel om hur stor andel av alla individer som har den aktuella egenskapen, hur unik egenskapen är och om egenskapen är permanent eller förändras över tid. Även hur lätt det är att samla in data om den aktuella egenskapen spelar in, liksom hur robust, träffsäker och accepterad tekniken är och hur lätt den är att kringgå, förfalska eller lura.[148]

146. https://aibusiness.com/machine-learning-and-biometrics-how-ai-is-becoming-more-human/.

147. https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.44, kap. 2.

148. http://oaji.net/articles/2019/2698-1549883755.pdf, sid. 3 958 och 3 961.

Utvecklingen går också fort framåt när det gäller beteendebaserad biometri. Tillämpningen har hittills baserats i huvudsak på inlärda beteenden, såsom hur vi använder ett tangentbord eller en mus, vår handstil och hur vi rör oss. En pågående utvecklingstrend är att istället studera mer reflexmässiga beteenden och beteenden som bygger på kognition – viljestyrda processer, som handlar om individens kunskap, tänkande och minne. Några exempel på aktuella forskningsområden inom denna trend är[149]

- medvetna och omedvetna ansiktsuttryck (mäts via blinkningar, ögonrörelser, pupillernas storlek med mera),
- kognitiv belastning – hur stor ansträngning som krävs av individen för att ta emot och behandla viss information (mäts via EEG, ögonrörelser med mera)
- inhämtning av visuell information – hur individen söker och upptäcker visuell information (mäts via EEG, reaktionstider med mera)
- reaktion på specifika stimuli – exempelvis reaktion på fotografier av specifik/stor betydelse individen (mäts via EEG, ECG med mera)

Ett relativt nytt forsknings- och utvecklingsområde inom biometri handlar om att samla in och analysera information om en persons interaktioner och beteende i sociala media – och använda den informationen för att verifiera att individen är den denne utger sig för att vara. Genom att kartlägga en persons beteende till exempel i sociala nätverk, chatforum, bloggar, dataspel, meddelandeappar, fildelningstjänster kan man identifiera mönster som är unika för användaren – och som därmed kan användas för att identifiera personen. Mönstren kan exempelvis baseras på en analys av när användaren är uppkopplad (tider), hur/var/med vem personen interagerar, innehållet i interaktionerna (preferenser, sätt att uttrycka sig etcetera) och användarens strategier vid onlinespelande.[150]

Ett annat område där teknikutveckling sker är så kallad ”multimodal biometri”, vilket innebär att flera olika biometriska egenskaper kombineras vid identitetskontroll, för att uppnå ökad säkerhet och tillförlitlighet.[151] Det kan exempelvis röra sig om en kombination av ögon-, venmönster och handavtrycksigenkänning.[152]

Även så kallad ”friktionsfri biometri” blir allt vanligare, vilket innebär att biometriska uppgifter samlas in från individer utan att de behöver interagera aktivt med tekniken eller ens märker att biometrisk teknik används.[153] Det används bland annat för övervakning och verifiering av individers identitet på flygplatser.[154] Fördelarna är bland annat ökad snabbhet och bekvämlighet, men på bekostnad av uppenbara integritetsrisker.

5.3.5.2 Särskilda nyttor med biometri

Möjligheten att kunna identifiera en individ på ett snabbt, enkelt och relativt träffsäkert sätt – utan att behöva hantera personliga koder eller säkerhetsprodukter som kort och ”blippar” – medför stor nytta i många situationer och den övergripande trenden är att biometriska data används i större utsträckning inom allt fler samhällsområden. Forskningen kring DNA-analys har gått raskt framåt de senaste åren och i dag finns det en uppsjö av internationella tjänster riktade mot konsumenter som kan användas för att matcha DNA.[155] Vanliga användningsområden för DNA-analys handlar till exempel om släktforskning, att utreda sitt ursprung eller olika hälsoutredningar. Andra exempel på hur biometrisk data används är biometriska ID-kort inom hela EU-området, biometrisk incheckning på flera av de största flygplatserna, kameror och ansiktsigenkänningsteknik för att bevaka storstäder och utbyte av biometrisk information mellan EU-länder är några exempel.

De mest uppenbara nyttorna med biometri – ur användarens perspektiv – är ökad bekvämlighet, snabbhet och säkerhet. Användaren behöver inte längre komma ihåg, eller löpande byta ut, krångliga lösenord. Glömda eller avmagnetiserade passerkort och ”blippar” är inte längre ett problem. Med biometri kan verifieringen i vissa fall ske utan att slutanvändaren behöver göra någonting alls, exempelvis i de fall då kameror och andra sensorer samlar in uppgifterna på distans. Ofta går den biometriska verifieringen också betydligt snabbare än att mata in lösenord, vilket bland annat fått många smarttelefonanvändare att övergå till fingeravtrycks- eller ansiktsigenkänning.

149. https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.44, kap. 2.2.2.
150. https://books.google.se/books?id=WIM7DwAAQBAJ&pg=PA3&lpg=PA3&dq=%22cancelable+biometrics%22+%22artificial+biometrics-%22&source=bl&ots=1ribUC1UTe&sig=ACfU3U3EJn0tS5hh46pF-F4-hr6NwfcpbZw&hl=en&sa=X&ved=2ahUKEwiXqrHyjoHpAhVOx4sK-HXCEC50Q6AEwA3oECAkQAQ#v=onepage&q=%22cancelable%20biometrics%22%20%22artificial%20biometrics%22&f=false, sid.2-5.
151. https://www.intechopen.com/online-first/multimodal-biometrics-for-person-authentication.
152. https://www.intechopen.com/online-first/multimodal-biometrics-for-person-authentication.
153. https://www.sciencedirect.com/science/article/abs/pii/S0969476517301558.
154. https://www.independent.co.uk/travel/news-and-advice/airport-biometrics-trial-face-recognition-klm-brisbane-sita-a7813271.html.
155. https://digital.di.se/artikel/dna-boomen-ar-pa-vag-till-sverige.

Säkerheten kan också förbättras såtillvida att användaren kan minska eller helt undvika bland annat risker som att någon smygtittar över axeln när ett lösenord matas in, passerkort eller en ”blipp” stjäls eller förloras eller att någon spärrar användarens passerkort och begär ut ett nytt i användarens namn. Säkerheten kan också motverka falska log-in-skärmar eller hårdvara som installeras för att stjäla användarens lösenord eller överbelastningsattacker där någon medvetet matar in felaktiga lösenord upprepade gånger för att låsa en produkt eller mjukvara.[156]

Biometri skapar också nytta för verksamheter inom allt fler samhällsområden. Speciellt där man har behov av att höja säkerhetsnivån vid åtkomst- eller tillträdeskontroller och önskar göra identifierings- och autentiseringsförfaranden säkrare genom att kombinera biometri med andra metoder, och inom sektorer där man önskar förenkla, snabba upp och öka bekvämligheten för den enskilde.[157]

Nedan ges exempel på användning och nyttor av biometri inom några av de sektorer där biometri hittills fått allra störst genomslag.

Inom offentlig förvaltning

- Fingeravtryck och biometrisk bildinformation inbyggt i ID-kort och pass, gör dessa svårare att förfalska.[158]
- Automatisk ansiktsigenkänning vid gränskontroller, gör det lättare att upptäcka eftersökta individer.[159]
- Kameraövervakning och ansiktsigenkänning vid av allmänna platser, gör övervakningen mer träffsäker och mindre personalkrävande.[160]
- Ansiktsigenkänning, fingeravtryck och DNA-analyser vid brottsutredningar är viktiga verktyg för att kunna identifiera misstänkta personer med stor träffsäkerhet.

Inom bank- och finanssektorn

- Röstigenkänning för att identifiera kunder som kontaktar banken via telefon, ersätter hantering av krångliga säkerhetsfrågor via telefonbanken och sparar tid både för banken och kunderna[161]
- Fingeravtrycks- och ansiktsigenkänning i bankomater och betalterminaler, ersätter PIN-koder och minskar därmed stölder och kortbedrägerier som banken annars måste lägga resurser på att utreda.[162]
- Tangenttryckningsmönster och rörelsemönster vid användning av mobila enheter, analyseras löpande för att identifiera avvikande beteenden och minska riskerna för bedrägerier.[163]

Inom hälso- och sjukvården

- IoT och bärbara sensorer, för att samla in och analysera patienters biometriska data i syfte att löpande bevaka patientens hälsotillstånd på distans, smittspårning med mera.[164]
- Fingeravtrycks-, retina- och ansiktsigenkänning, underlättar för vårdgivarna att kontrollera vem som ska ha tillträde till faciliteter och känslig information.
- Fingeravtrycks- och venmönsterigenkänning, för att på ett enklare och mer träffsäkert sätt identifiera patienter och hålla koll på patienten när den flyttas mellan olika verksamheter och avdelningar.[165]
- Fingeravtrycksigenkänning, för att förhindra bedrägerier kring sjukersättningar och mediciner.[166]

Inom it och telekommunikation

- Fingeravtrycks- och ansiktsigenkänning, i mobila enheter för snabbare och säkrare identifiering och accesskontroll till enheter och i mobila applikationer.
- Biometriska sensorer och IoT, för accesskontroll och identifiering i smarta fordon och på platser där fast internetuppkoppling inte är tillgänglig.
- ”Biometrics as a service”, tillgängliggör biometriska lösningar som en tjänst vilket gör tekniken både billigare och snabbare att implementera och ställer inte samma krav på expertkunskaper hos användaren.[167]

Det finns med andra ord ett stort antal områden där nyttan kan vara stor med att använda biometriska uppgifter.

156. http://oaji.net/articles/2019/2698-1549883755.pdf, sid. 3 958.
157. https://www.regeringen.se/49c627/contentassets/13d9126efb-b94e2cb5b084132275f184/hur-star-det-till-med-den-personliga-integri-teten---en-kartlaggning-av-integritetskommitten-sou-201641, sid. 116.
158. https://www.biometricupdate.com/201904/standard-for-eu-bio-metric-id-cards-one-step-from-approval-after-passing-european-parli-ament.
159. https://www.gemalto.com/govt/coesys/eborder/entry-exit-system.
160. https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.
161. https://emerj.com/ai-sector-overviews/voice-speech-recogni-tion-banking/.
162. https://findbiometrics.com/topics/atm/.
163. https://www.paymentscardsandmobile.com/are-you-being-track-ed-behavioural-biometrics-being-implemented-by-banks-to-redu-ce-fraud/.
164. https://www.biometricupdate.com/202004/liechtenstein-to-provi-de-citizens-with-biometric-bracelets-to-contain-coronavirus.
165. https://www.biometricupdate.com/wp-content/uploads/2015/02/Biometrics-in-Healthcare.pdf, sid. 12.
166. https://www.biometricupdate.com/wp-content/uploads/2015/02/Biometrics-in-Healthcare.pdf, sid. 12.
167. https://www.biometricupdate.com/tag/biometrics-as-a-service.

5.3.5.3 Särskilda integritetsrisker med biometri

Samtidigt är det uppenbart att användningen av biometriska uppgifter medför betydande risker för den personliga integriteten. Ett lösenord kan enkelt ersättas med ett nytt om det skulle gå förlorat. Detsamma gäller för passerkort och liknande teknik för verifiering, autentisering och identifiering. Om individen förlorar kontrollen över sina biometriska personuppgifter kan de däremot inte enkelt ersättas. Integritetsskadorna kan i värsta fall bli permanenta och det är en aspekt som gör integritetsfrågor kring biometri extra brådskande.

I flera av intervjuerna som genomförts i arbetet med denna rapport framhålls utvecklingen och användningen av teknik kring biometri som ett av de viktigaste utvecklingsområdena som påverkat den personliga integriteten under de senaste tre åren. Som exempel nämns i intervjuerna teknik för ansikts- och taligenkänning som används av rättsvårdande myndigheter. De integritetsrisker som följer av en ökad användning av biometriska uppgifter framhölls av Integritetskommittén redan 2016.[168] Kommittén konstaterade att en ökad användning av olika biometriska tekniker i samhället riskerar att göra det mycket svårt att någonstans i det offentliga rummet kunna vara helt anonym. När kameror och annan utrustning i omvärlden kan läsa av och identifiera den enskildes kropp eller personliga beteende och koppla ihop de biometriska uppgifterna med uppgifter från andra datakällor blir detta avsevärt mycket svårare. Sammantaget ansåg kommittén att användningen av tekniker som involverar många och detaljerade biometriska uppgifter innebär en påtaglig risk för den personliga integriteten.

Ett antal händelser som fått stort utrymme i media de senaste åren kan exemplifiera och konkretisera riskerna ytterligare:

2018 – Kina lägger till gångstilsigenkänning till sitt övervakningsnätverk som innehåller uppskattningsvis 170 miljoner kameror. Systemet innefattar bland annat teknik för ansiktsigenkänning och AI och är kopplat till landets ”sociala kreditsystem”. Systemet, som ska vara fullt fungerande under 2020, övervakar och betygsätter medborgare baserat på deras beteende.[169] Tre nya förordningar antas om Schengens Informationssystem (SIS), som bland annat innebär att SIS kommer att kunna användas för fler ändamål än tidigare, att fler uppgifter kan registreras i SIS och att fingeravtryck i högre utsträckning ska kunna användas för att identifiera personer.[170]

168. SOU 2016:41 *Hur står det till med den personliga integriteten*, sid 116.

169. https://apnews.com/bf75dd1c26c947b7826d270a16e2658a.

170. https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2019/12/ds-201927/.

2019 – San Francisco blir den första amerikanska staden som förbjuder användning av ansiktsigenkänning. Tekniken får inte användas av lokala myndigheter, till exempel stadens transportmyndighet, eller av lokala brottsbekämpande myndigheter.[171] USA:s tull- och gränsskydd offentliggör att bilder på resenärer och deras registreringsskyltar har stulits i en cyberattack riktad mot en underleverantör.[172] Israeliska säkerhetsforskare påstår sig ha kommit över biometriska data till fler än en miljon registrerade personer, via en databas som ägs av företaget Suprema. Företagets biometritjänster används av bland annat polis, banker och försvarsmakten i flera länder.[173] Kinesiska säkerhetsexperter demonstrerar hur de kan överlista samtliga befintliga fingeravtrycksläsare på bara 20 minuter.[174] I Florida tillåts polisen använda dna-data från webbplatsen GEDmatch – en behandling som de 1,3 miljoner användarna inte godkänt.[175]

2020 – Tyska säkerhetsexperter upptäcker att över en miljon dokument med hälsouppgifter och medicinskt bildmaterial kopplade till patienter i Indien är åtkomliga via en felkonfigurerad, uppkopplad databas.[176] New York Times skriver ett reportage om företaget Clearview AI, som samlat in tre miljarder fotografier på nätet och behandlar dessa med avancerad AI-ansiktsigenkänningsteknik.[177] Svensk polis lyckas för första gången lösa en mordutredning genom att testa DNA-prov mot släktforskningsdatabaser. Polisens utvärdering visar att en del aspekter av arbetssättet behöver utredas mer, men utvärderingen utmynnar i slutsatsen att målet bör vara att detta arbetssätt ska bli ytterligare ett verktyg för polisen.[178]

En risk är att biometriska uppgifter behandlas för nya ändamål som är oförenliga med de ändamål för vilka uppgifterna ursprungligen samlades in. Exempelvis kan biometriska uppgifter om gångstil och ansikte användas inte bara för att identifiera enskilda, utan också för att identifiera oönskade beteenden eller särskilda behov hos enskilda.

171. https://www.bbc.com/news/technology-48276660.

172. https://edition.cnn.com/2019/06/10/politics/customs-and-border-protection-images-travelers-data-breach/index.html.

173. https://www.silicon.co.uk/security/cyberwar/biometrics-breach-not-so-big-suprema-280807.

174. https://www.forbes.com/sites/daveywinder/2019/11/02/smartphone-security-alert-as-hackers-claim-any-fingerprint-lock-broken-in-20-minutes/#79740fb46853.

175. https://www.sciencemag.org/news/2019/11/judge-said-police-can-search-dna-millions-americans-without-their-consent-what-s-next.

176. https://economictimes.indiatimes.com/tech/internet/german-firm-finds-one-million-files-of-indian-patients-leaked/articleshow/73921423.cms?from=mdr.

177. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

178. https://www.svt.se/nyheter/lokalt/ost/polisen-vill-fortsatta-med-slaktforskning-och-dna.

En annan risk är att fler biometriska uppgifter hanteras än vad som behövs för ändamålet, till exempel att hela fingeravtryck samlas in och lagras när det i själva verket hade varit tillräckligt att bara hantera vissa mätpunkter från fingeravtrycket. Detsamma kan inträffa när uppgifter om DNA inte bara möjliggör identifiering, utan även avslöjar något om den registrerades hälsotillstånd, sjukdomsbenägenhet eller etniska ursprung.

Ytterligare en risk är att biometriska uppgifter inte skyddas tillräckligt och som en följd av detta blir tillgängliga för aktörer som kan använda uppgifterna för exempelvis identitetsstöld eller olika former av bedrägerier och utpressning.

Det finns också en risk för att biometriska uppgifter kan användas utan att den enskilde känner till det eller lämnar sitt samtycke, till exempel vid publicering av bilder på nätet eller i sociala medier där det finns särskild programvara för ansiktsigenkänning. Idag kartläggs vårt digitala liv i form av till exempel vilka sökningar vi gör på internet, vilka sidor vi besöker och tidningar vi läser, vad vi handlar och vilka som är våra kontakter. Kombineras sådan webbläsardata med biometriska uppgifter som till exempel kroppstemperatur, blodtryck och puls skulle slutsatser kunna dras om till exempel vilka nyheter eller kontakter som får en individ att reagera på olika sätt. Denna typ av scenarier har fått vissa bedömare att utfärda kraftfulla varningar för omfattande insamling av biometriska uppgifter, och konstatera att en sådan datainsamling ”kommer att få Cambridge Analyticas hacking taktik att framstå som något från stenåldern”.[179]

Därtill bör nämnas risken för överutnyttjande av biometri när tekniken blir billigare, enklare och därmed mer lättillgänglig. Alla sammanhang kräver inte den höga precision som biometri kan erbjuda.

Cyberattacker är en risk för alla system som ska förhindra otillbörlig åtkomst och tillträde och lösningar baserade på biometri är inget undantag. Potentiella säkerhetshot kan handla till exempel om att förfalska uppgifter. Det går att replikera de flesta biometriska data med hjälp av exempelvis 3d-printteknik och högupplösta bilder. Sensorer som används för insamlingen av uppgifterna kan manipuleras på många olika sätt och angripare kan också återanvända gammal data – exempelvis ett fotografi som tidigare använts för ansiktsigenkänning. Om en angripare tar sig in i systemet som bearbetar insamlad data så kan det gå att påverka resultatet. Angripare kan också tillföra förfalskad information, avlyssna kommunikationen där insamlade data matchas mot lagrade mallar eller stjäla och förfalska mallar.

När det upptäcks att ett traditionellt lösenord har hackats kan användaren oftast enkelt byta lösenordet mot ett nytt och därefter få fortsatt tillgång eller tillträde till tjänsten. Om biometriska data hackas så kan det däremot medföra betydligt värre konsekvenser för den enskilde. Om en individs biometriska data – exempelvis venernas struktur under huden – har hamnat i orätta händer så kan denne inte ersätta den med annan data. De biometriska uppgifterna är beständiga, vilket ofta gör integritetsförlusten mycket svår att reparera. Förutom svårigheten att förändra de biometriska uppgifterna är de dessutom ofta svåra att hålla för sig själv. Ett ansikte, avtryck från fingrar eller ett rörelsemönster är något som hela tiden exponeras mot omvärlden.

En risk är att någon använder stulna uppgifter för att skapa en artificiell, fysisk kopia av de biometriska uppgifterna som kan användas vid tillträdes- eller åtkomstkontroll. En annan risk är att biometrisk data avslöjar känsliga uppgifter om den registrerade – exempelvis information om en medfödd sjukdom – som kan användas för att skada den enskilde.[180] Ytterligare en potentiell risk är att en biometrisk uppgift – som till exempel en venprofil – svartlistas, om det blir allmänt känt att den är hackad. Därmed kan personen komma att nekas tillträde till platser och åtkomst till produkter och tjänster som bygger på autentisering med hjälp av just venernas struktur under huden.

En rad åtgärder kan vidtas för att minska riskerna kring biometriska data. En grundläggande utgångspunkt är att ha en restriktiv hållning och bara använda biometriska uppgifter när det är absolut nödvändigt. Säkerhetsåtgärder som att säkerställa att sensorer inte kan manipuleras, säker lagring av mallar, kryptering och säkra kommunikationsvägar samt multifaktorsautentisering kan också minska riskerna. Andra riskminimerande åtgärder kan handla om att använda artificiell biometridata (som kan bytas ut).

Biometriska uppgifter betraktas som en särskild kategori av personuppgifter (så kallade känsliga personuppgifter) enligt dataskyddsförordningen. Det är som utgångspunkt förbjudet att behandla känsliga personuppgifter. Behandling av sådana uppgifter är tillåten om något av de undantag som anges i förordningen är tillämpligt, till exempel uttryckligt samtycke från den enskilde.[181] För den som behandlar denna typ av uppgifter gäller vidare bland annat att det vanligen krävs en högre säkerhetsnivå än för mer harmlösa personuppgifter. Behandling av biometriska uppgifter har också betydelse för riskbedömningen när personuppgiftsansvarig gör konsekvensbedömningar och kan vara avgörande för om personuppgiftsansvarig måste rapportera en personuppgiftsincident, då incidenter som omfattar biometriska uppgifter ofta medför en hög risk för enskilda.

179. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fed-cca75.

180. https://eprint.iacr.org/2004/106.pdf, sid. 1.

181. Artikel 9 dataskyddsförordningen.

Sammanfattningsvis har tekniken stor potential att lösa en rad olika samhällsutmaningar, men förändrar samtidigt spelreglerna för den personliga integriteten i grunden. Hamnar biometriska uppgifter i orätta händer kan integritetsskadan vara permanent, eftersom biometriska uppgifter inte, som ett lösenord, enkelt går att byta ut.

5.3.5.4 Särskilt om deep fakes

Avslutningsvis finns ett riskområde som förtjänar att omnämnas särskilt, så kallade deep fakes. Deep fake är en benämning på falsk information som så genomarbetad att den verkar äkta, även vid relativt omfattande granskning. Området omfattar bland annat ”konstgjord media” – filmer, ljudinspelningar och fotografier – som efterliknar verkliga personer. Tekniken bygger bland annat på användning av AI och djupinlärning. Med hjälp av filminspelningar, fotografier och ljudinspelningar – data som kan ha biometriskt innehåll – av en verklig person kan en AI-modell läras upp till att skapa konstgjorda återgivningar av personen som är så verklighetstrogna att de är svåra att särskilja från äkta. Deep fake-videor kan till exempel visa ansiktet eller kroppen på en ”riktig” person, som pratar med en röst som är mycket lik dennes faktiska röst och agerar och använder mimik på ett sätt som denna brukar göra i verkliga livet. Men ansiktet, kroppen, rösten och rörelserna skapas av AI-modellen.

Den brittiska regeringen har tagit fram en rapport om deep fakes och vilseledande information. En slutsats är att det inte räcker med lagstiftning för att hantera risker, det krävs även investeringar i ny teknik för att avslöja manipulationer. Den brittiska regeringen ser också behov av utbildningssatsningar för att höja kunskap om deep fakes bland medborgarna. Exempel på svensk forskning inom området är utveckling av en app som kan avslöja deepfakes.[182]

Det finns ännu ingen rättspraxis som rör dataskyddsförordningens eventuella tillämplighet på deep fakes. Det är uppenbart att upplärningen av AI-modellen omfattas av dataskyddsreglerna, eftersom stora mängder biometriska personuppgifter används i denna fas, men när modellen väl är upplärd behövs inte längre personuppgifterna. Då är det modellen som skapar ny data som efterliknar biometriska personuppgifter. Om deep fake-material är att betrakta som personuppgifter och om dataskyddsförordningen är tillämpbar på material skapat med deep fake-metoder är några av de rättsliga frågor som kommer att behöva prövas.[183]

182. Komet kommenterar 2020:27 *Deep fakes, manipulerade filmer – korta faktablad om aktuell teknik.*

183. Frågor som reses rör exempelvis hur en film som skapats helt artificiellt, baserat på publik biometrisk data (röst, utseende, rörelsemönster etc.) från bland annat sociala media, ska hanteras ur ett personligt integritetsperspektiv.

5.4 Teknik för att bearbeta och använda data

De ökade möjligheterna att samla in data skulle i praktiken vara värdelösa om inte tekniken för att bearbeta och använda uppgifterna också tagit stora utvecklingssprång.

Utvecklingen av *AI* är ett av de utvecklingsområden som haft störst påverkan på den personliga integriteten under de senaste åren. De potentiella nyttorna är stora och Sveriges mål är enligt den nationella inriktningen för AI att bli bäst i världen på att utnyttja AI:s möjligheter. I dagsläget använder ungefär 5 procent av svenska företag och 10 procent i offentlig sektor AI. Samtidigt innebär AI integritetsrisker för den enskilde i form av bland annat bristande transparens, diskriminering, försvårat ansvarsutkrävande, missbruk och fientlig användning. Särskilda risker finns vid automatiserade processer i beslutsfattande, när ett beslut kan få rättsliga konsekvenser för den enskilde.

En pågående förändring med potential att påverka integritetsskyddet positivt handlar om var data i bearbetas – i centrala datacentra och serverhallar eller lokalt. Teknik för *edge computing* medför att bearbetning av data nu allt oftare kan ske lokalt, i uppkopplade enheter med låg kapacitet eller i lokala servrar. Detta innebär att data i mindre utsträckning behöver transporteras och delas, vilket kan skapa bättre kontroll.

Ett av de områden där den omfattande bearbetningen av stora datamängder blir som mest uppenbar för många är den *digitala annonsmarknaden*. De komplexa och icke transparenta processerna som kan inkludera hundratals aktörer gör det i praktiken omöjligt för den enskilde att utnyttja sina rättigheter, till exempel att få information raderad. Såväl norska som brittiska myndigheter har i färska analyser kommit till slutsatsen att stora delar av den digitala annonsmarknaden systematiskt bryter mot dataskyddslagstiftningen.

De enorma informationsmängder som kan samlas in med hjälp av ny teknik skulle i praktiken vara värdelösa om inte tekniken för att bearbeta och använda uppgifterna också tagit stora utvecklingssprång. De senaste decenniernas utveckling av olika Big data-metoder har utgjort en viktig förutsättning för förmågan att hantera den faktiska mängden data. Centralt i de senaste årens utveckling är att AI och andra tekniker som tidigare var tillgängliga endast för resursstarka och specialiserade aktörer, tillgängliggörs nu på bred front, exempelvis via allt billigare och mer lättanvända molntjänster med stor kapacitet att behandla data. En mer komplex bearbetning av personuppgifter kan därmed genomföras av fler. Tekniska lösningar för att bearbeta data är inte i särskilt stor utsträckning beroende av användarens tekniska förkunskaper eller förståelse för hur tekniken påverkar integritetsskyddet.

Större datamängder kan bearbetas på kort tid och bearbetningen genererar resultat som tidigare inte var möjliga att uppnå. I allt fler fall sker bearbetningen av data med helt eller delvis automatiserade metoder, i självlärande system som kontinuerligt utvecklas och förfinas.

Tekniken skapar stor nytta och håller på att förändra flera branscher i grunden. Att anpassa och använda AI-lösningar på ett effektivt sätt spås bli en överlevnadsfråga inom många branscher. Drivkrafterna att snabbt implementera dem är därför mycket stark.

Både de stora volymerna personuppgifter som bearbetas med den nya tekniken, samt resultaten av bearbetningen, innebär nya integritetsutmaningar. Några av dem behandlas i det följande.

5.4.1 Artificiell intelligens

Utvecklingen av artificiell intelligens, AI, har gjort stora framsteg under de senaste åren och dess potential är på många områden lovande. Sedan begreppet AI först användes på femtiotalet har tekniken fått en allt större spridning. Förklaringarna finns bland annat i mer sofistikerade algoritmer, väsentligt ökad beräkningskapacitet och allt fler användningsområden inom såväl näringsliv som samhälle. En annan orsak är utveckling av hårdvara i datorer, vilken möjliggör snabb hantering av stora datamängder. Till exempel kan dagens AI system gå igenom tusentals patientjournaler på några sekunder. Slutligen har såväl modeller som algoritmer utvecklats över tid, vilket medfört att data kan komma till användning på fler, och mer kraftfulla, sätt.[184]

184. Komet informerar 2020:30; *Den nya tekniken – så fungerar den.*

Regeringen har i den nationella inriktningen för artificiell intelligens från 2018 slagit fast att Sverige ska vara ledande i att ta tillvara möjligheterna som användning av AI kan ge, med syftet att stärka både den svenska välfärden och den svenska konkurrenskraften. Ett genomgående tema bör enligt den nationella inriktningen vara hållbarhet, med innebörden att AI-applikationer bör vara etiska, säkra, pålitliga och transparenta. Etiska och säkerhetsmässiga överväganden kan enligt regeringen inte vara en eftertanke i AI-applikationer, utan måste vara en integrerad del från det tidiga designarbetet.[185]

I de intervjuer som IMY genomfört framhålls AI som ett av de utvecklingsområden som varit mest aktuella och haft störst påverkan på den personliga integriteten under de senaste tre åren.

5.4.1.1 Vad är AI?

Begreppet AI har ingen entydig definition eller allmänt vedertagen avgränsning. Oftast används termen som ett paraplybegrepp för teknik som kan lära av sina egna erfarenheter, bli smartare över tid och mer eller mindre självständigt lösa komplexa problem i olika situationer. Vinnova definierar AI som *förmågan hos en maskin att efterlikna intelligent mänskligt beteende*.[186]

Statistiska Centralbyrån, SCB har i en rapport definierat AI som *system som uppvisar intelligent beteende genom att analysera sin omgivning och agera, med någon nivå av självbestämmande, för att uppnå specifika mål.* AI-baserade system kan vara ren mjukvara eller inbyggda i hårdvara.[187]

Den stora uppmärksamhet som AI fått globalt de senaste åren beror framför allt på en ökad användning av maskininlärning i olika tillämpningar. Maskininlärning är teknik som gör det möjligt för datorer att ”tänka” och bli smartare över tid. Genom att skapa matematiska algoritmer baserade på omfattande mängder data drar systemet slutsatser, lär sig och bygger nya algoritmer – utan att en människa behövt ge programmet den specifika instruktionen. Utvecklingen inom maskininlärning har gått mycket fort framåt de senaste åren, bland annat till följd av den ökade tillgången på större datamängder samt större och billigare processorkraft och lagringskapacitet.

Vissa typer av maskininlärning bygger på samma principer som den mänskliga hjärnans nervnätverk med ett inmatningsskikt, ett eller flera dolda lager och ett utgående lager. Om det finns mer än ett dolt lager talar man om djupinlärning. Ofta används även termen neurala nätverk för denna typ av maskininlärning. Antalet lager i ett neuralt nätverk kan variera, men som exempel kan nämnas att Microsoft 2016 vann en tävling i bildigenkänning med ett nätverk bestående av 152 lager.[188]

Samtidigt som AI är en förutsättning för att förädla och dra nytta av stora datamängder är AI-algoritmerna beroende av stora datamängder för att läras upp. Begreppen AI och big data är därför nära förknippade med varandra. Big data, som på svenska ibland översätts till stordata eller stora data, syftar på mycket stora datamängder som kräver speciella metoder för analys. Uttrycket syftar oftast på ostrukturerade data, som inte kan ordnas i tabeller eller kalkylark. Datamängderna är så omfattande att de i praktiken inte kan bearbetas med traditionella program för analys och datautvinning. Big data kan ha många olika format och komma till exempel från sociala medier och webbplatser (till exempel Facebook, Youtube bloggar, foton och videofilmer), företagssystem (till exempel transaktioner, kundregister, kreditkortsdata och medicinska register) och IoT (till exempel sensordata om väder, trafik, mobiltelefoner och satellitbilder). Vissa bedömare menar att själva tekniken för AI (till exempel maskininlärning) och data är så intimt förknippade med varandra att en definition av AI bör inkludera båda dessa huvudkomponenter; algoritmer och data.[189]

Även om begreppet AI ibland används synonymt med maskininlärning och djupinlärning finns även andra typer av AI-teknik. Det kan handla om system som gör det möjligt för datorer att förstå hur olika typer av begrepp hör ihop och ska sorteras hierarkiskt (eng. *ontology engineering*) eller system som gör det möjligt för datorer att hantera värden mellan ja och nej (eng. *fuzzy logic*).[190]

5.4.1.2 Utveckling hittills av AI och dess potential i Sverige

I en kartläggning av Vinnova som presenterades 2018 konstaterades att tillämpningar av AI redan haft stor betydelse för utveckling av internetplattformar, informationssökning, bildigenkänning och automatöversättning. Samtidigt hade det praktiska genomslaget för AI enligt Vinnova varit begränsat i stora delar av näringslivet och inom offentlig verksamhet i Sverige.[191]

185. Näringsdepartementet; *Nationell inriktning för artificiell intelligens*, https://www.regeringen.se/49a828/contentassets/844d30fb0d594d1b-9d96e2f5d57ed14b/2018ai_webb.pdf

186. Vinnova rapport 2018:08 *Artificiell intelligens i svenskt näringsliv och samhälle – Analys av utveckling och potential*

187. Statistiska Centralbyrån (SCB) *Artificiell intelligens i Sverige.*

188. Datatilsynet; *Kunstig intelligens og personvern*, 2018.

189. COM (2020) 65 *Vitbok om artificiell intelligens - en EU-strategi för spetskompetens och förtroende.*

190. Vinnova rapport 2019:5, *AI-miljöer i Sverige En översikt över miljöer som bidrar till utvecklingen av artificiell intelligens.*

191. Vinnova rapport 2018:8, *Artificiell intelligens i svenskt näringsliv och samhälle – Analys av utveckling och potential.*

Sverige har sedan dess inrättat ett nationellt center för artificiell intelligens, AI Sweden, som finansieras i samverkan mellan offentlig och privat sektor. Centret arbetar för att påskynda användningen av AI till förmån för samhället, svensk konkurrenskraft och landets invånare.[192]

Statistiska centralbyrån, SCB redovisade i november 2020 ett regeringsuppdrag att kartlägga användningen av AI samt analys av stora datamängder i Sverige.[193] Kartläggningen visade att användning av AI är vanligare inom offentlig än i privat sektor. Bland privata företag uppgav 5,4 procent att de använt AI i någon form i sin verksamhet under 2019, medan motsvarande siffra inom den offentliga sektorn var 10,2 procent. Den vanligaste anledningen att använda AI var bland företag att förbättra en existerande produkt eller tjänst, medan det i offentlig sektor var vanligast att använda AI för att förbättra interna processer. När det gäller hinder för att använda AI uppgav privat sektor att kostnad för tjänster eller utrustning utgjorde det största hindret för användning av AI. Inom offentliga sektorn utgjorde istället anställdas kompetens, utbildning eller erfarenhet det största hindret.

Vinnova har i flera sammanhang understrukit att regulatorisk utveckling när det gäller data och datatillgång kommer att vara av avgörande betydelse för Sveriges AI-utveckling.[194] Fundamentala behov av tillgång till data behöver balanseras med integritetsskydd, etik, tillit och samhällsskydd. Ett sätt att driva regulatorisk utveckling är enligt Vinnova att relevanta aktörer med expertis och ansvar för reglering och regelövervakning bör medverka i innovationsprocesser där nya AI-tillämpningar utvecklas.

Även DIGG framhåller regulatorisk utveckling som en framgångsfaktor för att främja AI-tillämpningen. I en rapport från januari 2020 om AI i offentlig sektor konstaterade DIGG att det finns stor potential för offentlig förvaltning att använda AI men att det också krävs att ett antal förmågor utvecklas.[195] Förmågor som behöver utvecklas är till exempel tydligare styrning och ledning, ändamålsenlig rättsutveckling, bättre förutsättningar för kompetensförsörjning, gemensam digital infrastruktur (teknik och data), data som strategisk resurs och ekosystem för samarbete och innovation.

Bland de förslag som DIGG anser bör prioriteras först ingår att inrätta ett förfarande eller en mekanism för att ta fram författningsstöd för försöksverksamhet, eftersom det skulle kunna stimulera offentlig förvaltning till att genomföra försök med att använda AI. De regulatoriska sandlådor som prövats i bland annat Storbritannien framhålls av DIGG som ett gott exempel. För att underlätta en ändamålsenlig rättsutveckling föreslog DIGG också etableringen av rättsligt beredningsorgan – ett förslag som tidigare lämnats av Digitaliseringsrättsutredningen 2018.

5.4.1.3 Exempel på nyttor och risker med AI

AI-teknik kan tillämpas på en rad olika områden. Bland de samhällsutmaningar som AI kan bidra till att lösa finns till exempel bättre förmåga att upptäcka, diagnostisera, förebygga och behandla allvarliga sjukdomar, ett mer effektivt jordbruk, nya metoder för klimat- och miljöskydd, minskad energianvändning, färre trafikolyckor, en bättre och mer effektiv offentlig sektor och ett säkrare samhälle.

Exempel på vanliga uppgifter för ett AI-system är att välja den bästa åtgärden eller föreslå det bästa handlingsalternativet givet ett specifikt mål. Uppgiften kan exempelvis innefatta mönsterigenkänning, bildanalys, talförståelse, prediktiv analys skapande av bevis och spel. Systemet lär sig vilken åtgärd som ska vidtas eller vilket handlingsalternativ som ska rekommenderas genom att ta in och bearbeta data och lära upp algoritmer som är anpassade till det specifika ändamålet.

Ett särskilt användningsområde handlar om olika system för automatisering och intelligent automatisering där mjuk- eller hårdvara utvecklas för att kunna fungera autonomt, utan att behöva styras eller kontrolleras av en människa. Det som automatiseras kan exempelvis vara informationsbearbetning, utförande av uppgifter och beslut. Intelligent automatisering innebär att automatiseringen är AI-baserad, med helt eller delvis autonoma system som är självlärande och som kan bearbeta stora mängder data.[196]

Intelligent automatisering och robotisering spänner över ett stort antal sektorer och innebär bland annat att personuppgifter behandlas på nya sätt och på fler platser. Exempel på sektorer där teknikutveckling genom automatisering pågår är hälsovård, konsumentprodukter, polis och rättsväsende, samt logistik och transport.[197]

192. https://www.ai.se/en/about-aisweden
193. Statistiska centralbyrån (SCB) *Artificiell intelligens i Sverige*.
194. Se till exempel Vinnova rapport 2018:8, *Artificiell intelligens i svenskt näringsliv och samhälle – Analys av utveckling och potential*.
195. Myndigheten för digital förvaltning (DIGG) *Främja den offentliga förvaltningens förmåga att använda AI*. Delrapport i regeringsuppdrag I2019/01416/DF och I2019/01020/DF.
196. https://www.mckinsey.com/featured-insights/future-of-work/ai-automation-and-the-future-of-work-ten-things-to-solve-for.
197. https://www.eu-robotics.net/cms/upload/downloads/ppp-documents/Multi-Annual_Roadmap2020_ICT-24_Rev_B_full.pdf.

Nedan listas kortfattade exempel på konkreta användningsområden för AI inom olika sektorer som ger en bild över olika tillämpningsområden och potentialen med utvecklingen inom olika sektorer.[198]

- **Hälso- och sjukvård** – automatiska/bildbaserade diagnoser och dialogrobotar. Utvecklade datorprogram som ska kunna föra en ändamålsenlig dialog med människor, till exempel svara på frågor.[199]
- **Offentlig sektor** – effektivisering av arbetsflöden, automatisering av beslutsgångar och prediktion, att kunna förutse vad som kommer att hända.[200]
- **Cybersäkerhet** – automatiserad realtidsanalys av stora system och flera parallella säkerhetshot.[201]
- **Försäkring** – automatiserad riskbedömning och upptäckt av försäkringsbedrägerier.
- **Finans** – roboträdgivare och automatiserade beslutsstöd baserade på kunddata och annan data som företagen har tillgång till.
- **Bioteknik** – analys av mycket stora datamängder och prognostisering.
- **Handel** – analys och förståelse av kundbeteenden för att förutsäga framtida köpbeteenden och anpassa erbjudanden.
- **Tillverkande industri** – automatiserad diagnos och kvalitetskontroll.
- **Telekommunikation** – optimering av nätverk och förstärkt cybersäkerhet.
- **Transport** – säkerhetsfunktioner genom löpande övervakning och analys av förarens beteenden och uttryck.
- **Underhållning** – filmmanus och musik som skapas via djupinlärning baserad på personlig data och marknadsdata.

Samtidigt som AI rymmer stora möjligheter i de flesta sektorer aktualiserar utvecklingen både rättsliga utmaningar, säkerhetsfrågor och etiska dilemman. Riskerna för enskildas fri- och rättigheter innefattar bland annat bristande transparens, diskriminering, försvårat ansvarsutkrävande eller missbruk och fientlig användning men också risken för felaktig programmering av algoritmer, som leder till felaktiga eller snedvridna beslutsunderlag. Vissa av dessa risker beskrivs ytterligare i avsnitt 7.1.7 som ger exempel på forskning om AI.

198. https://www.startus-insights.com/innovators-guide/insurtech-innovation-map-explains-emerging-technologies-startups/.

199. https://en.wikipedia.org/wiki/Artificial_intelligence_in_healthcare.

200. https://www.arbetsgivarverket.se/nyheter--press/nyheter/2018/lunchforelasning-ai/.

201. https://towardsdatascience.com/cyber-security-ai-defined-explained-and-explored-79fd25c10bfa.

Kommittén för teknologisk innovation och teknik (Komet) har i en kommentar om AI betonat urvalets betydelse för etisk träning av algoritmer vid maskininlärning. Om träningsdata inte är neutrala och rättvisande finns en risk för snedvridning och systematiska fel.[202]

De stora datamängder som kan analyseras med AI medför att enskildas kontroll över sina personuppgifter försvagas och ansvarsfrågor blir komplexa. Vem ska hållas ansvarig om en diagnos eller ett beslut som fattats med hjälp av AI blivit fel? Den som skapat algoritmerna, den som matat in data eller den som tillämpat AI-lösningen? När en personuppgiftsincident inträffar kring big data kan också mycket stora mängder uppgifter förloras och ett stort antal registrerade individer drabbas.

Den ökade förmågan att finna samband i stora datamängder innebär också att det blir allt svårare för konsumenter att värdera vilka typer av data som är särskilt känsliga och i vilka sammanhang. När stora datamängder samkörs och analyseras ökar förmågan att identifiera individer även utifrån data som inte ursprungligen utgör personuppgifter, exempelvis med stöd av appar eller rörelsemönster som samlats in med IoT. Därmed utökas successivt integritetsskyddsområdet.

Särskilda risker finns vid automatiserade processer i beslutsfattande, när ett beslut kan få konsekvenser för den enskilde. I dataskyddsförordningen begränsas möjligheten att fatta beslut som enbart grundar sig på automatiserad behandling (inklusive profilering).[203] Det finns flera risker kopplade till automatiskt beslutsfattande, bland annat hur man säkerställer förfaranden som är rättssäkra och möjliggör att man kan uppmärksamma och utreda fel i bakomliggande tekniska förfaranden.[204] I förordningen betonas vikten av att automatiskt beslutsfattande omgärdas av lämpliga skyddsåtgärder och transparens, bland annat information till den registrerade, rätt till mänskligt ingripande och rätt att få en förklaring till beslutet.[205]

202. Ett välkänt exempel är experimentet The moral machine från 2018 som undersöker moraliska dilemman för självkörande fordon. I experimentet studeras hur etiska principer till grund för styrning av maskiner varierar mellan olika länder och kulturer och om ställningstagande i ett dilemma skiljer sig åt beroende på kön, ålder eller inkomst. Experimentet illustrerar vikten av insyn i vilka data som använts för att träna en algoritm, för att kunna bedöma hur maskinen kommer att bete sig i ett skarpt läge. Komet lyfter bland annat fram att det kan finnas utmaningar med system som byggs i ett land med vissa preferenser, säljs i ett annat och används i ett tredje. Komet informerar 2020:30; *Den nya tekniken – så fungerar den*.

203. Artikel 22 dataskyddsförordningen. Även förvaltningslagen innehåller en bestämmelse om automatiskt beslutsfattande, 28 §.

204. SOU 2018:25 *Juridik som stöd för förvaltningens digitalisering*.

205. I beaktandesats 71 till dataskyddsförordningen anges att tekniska och organisatoriska åtgärder ska vidtas som bland annat säkerställer att risken för fel minimeras och att personuppgifterna säkras genom att diskriminerande effekter förhindras.

Även strukturer som bygger på mänskliga bedömningar kan resultera i systematiska fel, till exempel om en verksamhet har undermåliga rutiner eller fel kompetens hos dem som handlägger ärenden. Kännetecknande för fel eller brister i ett automatiserat förfarande är dock att de på kort tid kan reproduceras i stor skala.

I Australien har det så kallade Robodept-fallet väckt stor uppmärksamhet och nationell frustration kring automatiserade beslut. AI-lösningen Robodept introducerades 2015 med syftet att upptäcka bedrägerier i välfärdssystemet. Systemet jämförde automatiskt de inkomstuppgifter som redovisades av bidragstagare med uppgifter från skattemyndigheten. Upptäcktes diskrepanser registrerades en skatteskuld automatiskt. Eftersom algoritmen inte beaktade den stora volatiliteten i många låginkomsttagares inkomst ledde systemet till att tusentals australiensare felaktigt fick skatteskulder registrerade och krävdes på pengar. I ett par fall hävdar anhöriga att denna motgång blev så tung för de enskilda att det utlöste självmord. Det numera nedlagda systemet har varit föremål för ett mycket stort antal utredningar, rättsprocesser och parlamentariska utfrågningar i Australien.[206]

I Sverige upptäckte Arbetsförmedlingen vid en intern kontroll 2019 att mer än vart sjunde beslut om indraget aktivitetsstöd kan ha varit felaktigt till följd av brister i ett automatiserat system. Potentiellt bedömdes tiotusentals beslut ha blivit fel under den tid som systemet var i drift.[207]

5.4.2 Edge computing

Edge computing översätts ibland på svenska till ”databehandling i utkanten av nätverken”. Även benämningar som ”decentraliserad AI” eller ”federated learning” förekommer. Mer konkret innebär edge computing att ny bearbetning av data sker direkt i enheten, ofta i utkanterna av ett nätverk. Det kan till exempel handla om avancerad kamerateknik som samlar in data, men också krypterar, lagrar och bearbetar data lokalt och i realtid, utan att behöva transportera den via nätet till en central server eller dator. Edge computing kan också handla om att data är lokaliserad i lokala nätverk, till exempel på ett antal sjukhus, och decentraliserade algoritmer placeras ut lokalt för att träna på datan. Olika lokala algoritmer förs sedan samman i en central lösning. Därmed kan algoritmer tränas på stora datamängder utan att själva datan behöver centraliseras eller delas, vilket förespråkarna menar skulle kunna vara ett sätt att möta dataskyddsförordningens krav.[208]

206. https://www.bbc.com/news/world-australia-54970253.

207. https://www.svt.se/nyheter/inrikes/svt-avslojar-stort-data-fel-hos-arbetsformedlingen-tusentals-kan-ha-forlorat-ersattning.

208. https://www.ai.se/en/node/81535/federated-learning

I den vitbok om AI som EU-kommissionen publicerade 2020 förutspås att vi kommer att se en stor förändring i bearbetningstekniker inom de närmsta åren. Idag sker 80 procent av bearbetningen och analysen av data i datacenter och serverhallar och ungefär 20 procent i uppkopplade enheter, till exempel i bilar eller i uppkopplade prylar i hemmet. Till 2025 förutspås att relationerna är de omvända.[209]

Nyttorna med bearbetning av data genom edge computing anses bland annat vara följande.[210]

- Ökad hastighet och minskad fördröjning i bearbetningen av insamlad data vilket möjliggör beslut i realtid.
- Ökad driftsäkerhet.
- Ökade möjligheter att hantera IoT-enheter centralt från molnet och använda enheterna utan anslutning eller med tillfällig anslutning.
- Reducerade bandbreddskostnader.
- Ökad säkerhet och kontroll på data, eftersom den kan krypteras och bearbetas lokalt och inte behöver transporteras för att bearbetas någon annanstans.

Edge computing är bland annat en viktig förutsättning för den fortsatta utvecklingen av autonoma fordon. För att autonom körteknik ska ersätta mänskliga förare måste fordonen kunna reagera på incidenter och avvikelser, exempelvis en trafikolycka, i realtid. I genomsnitt kan det ta 100 millisekunder för dataöverföring mellan fordonsensorer och ett molnbaserat datacenter, vilket när det gäller körbeslut kan vara för lång tid. Genom att data kan bearbetas och analyseras lokalt i fordonet snabbas tekniken upp väsentligt.

Teknik som 5G och AI banar ytterligare väg för edge computing. 5G hjälper till att distribuera datorkapacitet till enheter i utkanten av nätverket och AI skapar förutsättningar för beslutsfattande i realtid.[211]

Teknikutvecklingen inom detta område innebär risker, bland annat om lokal bearbetning sker i enheter med låg säkerhet. Men det innebär också möjligheter för den personliga integriteten, bland annat beroende på vilken bearbetning som görs och i vilka syften, hur säker data är i enheten där den bearbetas, samt vilken kontroll den registrerade själv ges över sina personuppgifter.[212] Tekniken kan medföra att individen får bättre kontroll på sina personliga data, om den bearbetas i den egna enheten (exempelvis den egna telefonen) eller i ett lokalt nätverk och aldrig transporteras därifrån.[213]

209. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

210. https://techworld.idg.se/2.2524/1.683223/edge-computing.

211. https://www.bmc.com/blogs/edge-computing/.

212. https://www.zdnet.com/article/edge-computing-the-cyber-security-risks-you-must-consider/.

213. https://blog.westerndigital.com/designing-edge-5-trends-smart-security/.

5.4.3 Den digitala annonsmarknaden och realtidsbudgivningar

Ett av de områden där den omfattande bearbetningen av stora datamängder blir som mest uppenbar för många är den digitala annonsmarknaden. De flesta människor som använder sociala medier har idag personliga erfarenheter av hur en viss sökning på Internet eller ett besök på en viss webbsida resulterar i att annonser på samma tema kort därefter syns i nyhetsflödet.

Den digitala annonsmarknaden omsätter enorma belopp. Under 2019 spenderades globalt omkring 330 miljarder dollar på den digitala annonsmarknaden, vilket var en ökning med drygt 17 procent jämfört med året innan.[214] Samtidigt sker merparten av den digitala datainsamlingen av personuppgifter utan att den enskilda individen förstår eller är medveten om det. Processerna kring insamling, analys, samkörning, profilering och försäljning av personuppgifter till tredjepartsaktörer är komplexa och för den enskilde individen är det i stort sett omöjligt att förstå och påverka hur de egna personuppgifterna används.

En bidragande förklaring till komplexiteten är det stora antalet aktörer som är involverade i den digitala annonsmarknaden (så kallad AdTech). Dagens internet genomsyras av komplicerade nätverk av aktörer som samlar in, köper, säljer, förmedlar, förädlar och analyserar data på olika sätt för en mängd olika syften.

Norska konsumentskyddsmyndigheten Forbrukerrådet publicerade i början av 2020 en omfattande kartläggning av den digitala annonsindustrin.[215] I undersökningen granskades tio vanliga Android-appar. Bedömningen var att AdTech-sektorn utnyttjar stora mängder data från apparna, som överför data till en stor mängd tredjepartsaktörer. Det var i olika kombinationer frågan om överföring av persondata, ibland känsliga personuppgifter, GPS-koordinater, IP-adresser, Wi-Fi accesspunkter och i något fall en lista över installerade appar i användarnas telefoner. Av rapporten framgår vidare att det också förekom en omfattande möjlighet att sammanställa information från olika enheter, exempelvis från mobil, dator och laptop. De enskilda hade sällan kunskap eller kännedom om att deras data fördes vidare till tredjepartsaktörer. Var och en av apparna delade data med flera tredjeparter och de undersökta tio apparna överförde tillsammans användardata till minst 135 tredjepartsaktörer för användning i marknadsföring eller beteendeprofilering (i första ledet). Rapportens slutsats är att AdTech-sektorn delar och behandlar data helt ”out of control”.

Den omfattande spårningen och profileringen av konsumenter är enligt undersökningen till sin natur explorativ. Det saknas insyn och transparens vilket gör konsumenterna sårbara för manipulation, särskilt då för dem helt okända företag har mycket omfattande kunskap om dem. Systemet bygger idag enligt Forbrukerrådet helt på användning av illegalt insamlad persondata. Medborgarna har små eller inga möjligheter att skydda sig mot exploateringen av deras uppgifter och den genomgripande profileringen. Alternativet är ofta att helt avstå från att använda en viss app. Affärsmodellerna behöver ändras i grunden om aktörerna inom AdTech-sektorn ska uppfylla kraven enligt dataskyddsförordningen och respektera konsumenters grundläggande fri- och rättigheter.

I rapporten delas aktörerna på den digitala annonsmarknaden in i fyra större huvudkategorier; publicister, annonsörer, tredjepartsaktörer och de större plattformsföretagen. Gränserna mellan aktörernas verksamheter kan i vissa fall vara otydliga.

- **Publicister** – består av alla typer av webbsidor och mobilappar som tillhandahåller information och interaktiva tjänster till användarna. Publicisterna erbjuder annonsplatser och kan samtidigt sälja användardata.
- **Annonsörer** – vill främst erhålla nya men även behålla befintliga kunder och finns till exempel inom detalj- och dagligvaruhandeln, researrangörer, telekombolag och säljare av finansiella tjänster.

Utöver publicister och annonsörer, som har direktkontakt med användarna, finns ett antal aktörer som kunder och besökare på webbplatser inte kommer i kontakt med.

- **Tredjepartsaktörer** – kan vara annonsnätverk, analysföretag och datamäklare (databrokers) som på olika sätt är involverade i den digitala annonsmarknaden. Aktörerna hanterar och processar stora mängder personuppgifter, men varken publicister eller annonsörer har någon större kontroll över hur datan hanteras och används.
- **Plattformsföretag** som Google och Facebook – har multipla roller i industrin och kan agera som både publicister och tredjepartsaktörer. Google och Facebook är centrala och dominerande aktörer i den digitala annonsindustrin eftersom de kontrollerar stora delar av leveranskedjan av personuppgifter.

214. https://www.emarketer.com/content/global-digital-ad-spending-2019.

215. Forbrukerradet *Out of control, How consumers are exploited by the online adversiting industry*, sid. 23.

5.4.3.1 Hur fungerar den digitala annonsindustrin i praktiken?

Varje gång en individ besöker en webbsida eller använder en mobilapp, sänds information till publicisten, men även till ett stort antal tredjepartsaktörer. Förfarandet kallas spårning eller tracking. Den vanligaste spårningsmetoden är genom kakor (eng. cookies), vilket är små textfiler som webbplatsen skickar till användarens webbläsare. Filen sparas i användarens dator, antingen bara under tiden användaren besöker webbplatsen (så kallad sessioncookie) eller för en längre tid. Varje gång användaren besöker en viss webbsida skickas innehållet i dessa kakor med. På så vis kan webbplatsen identifiera och komma ihåg användaren.

Om webbplatsen har ett avtal med en tredje part (till exempel Google eller Facebook) kan tredjeparten sätta en egen kaka ("tredjepartskaka") på webbplatsen. Denna kaka kommer sen att skickas till tredjepartsaktören även när användaren besöker andra webbplatser som använder sig av samma tredjepart. På så vis kan tredjeparter kartlägga, eller "följa", användare mellan olika webbplatser och ta fram profiler utifrån vad användaren gör.

Kakor är den vanligaste, men inte den enda metoden för att spåra och identifiera användare på nätet. Eftersom kakor är förhållandevis enkla att ta bort och blockera har det nu också utvecklats mer sofistikerade spårningsmetoder, till exempel via digitala fingeravtryck som tas fram genom att kombinera ett antal datapunkter om en individ. Det kan handla till exempel om användarens webbläsare, operativsystem, skärmstorlek, språkinställning, tidszon, installerade typsnitt och insticksprogram, hårdvara och mycket annat.[216]

Konkurrensverket har nyligen låtit göra en kartläggning av spårningen med kakor på ett antal svenska webbplatser.[217] Kartläggningen omfattade 116 webbplatser inom branscherna media, handel, bank/försäkring, hälsa och offentlig sektor. Resultatet visade att de flesta webbplatsbesök medför att en stor mängd tredjeparter samlar in data och spårar besöket, om inte särskilda åtgärder tagits av användaren för att förhindra detta. Flest tredjepartsaktörer fanns på webbplatser inom media, där varje besök på en webbplats i genomsnitt ledde till att 35 tredjepartsaktörer kontaktades. Motsvarande siffra för andra branscher var inom handeln 17, bank/försäkring 10, hälsa 9 och offentlig sektor 6.

Tredjepartsaktörer tillhandahåller olika tjänster, och kan därmed antas använda informationen från tredjepartskakor på olika sätt. Vissa aktörer erbjuder system som möjliggör att en annons visas för en viss konsument eller ett visst segment av kunder vid ett visst tillfälle.

En särskild kategori tredjepartsaktörer är datamäklare som samlar in data från en mängd olika källor, både offline och online och där uppgifterna inte alltid är användargenererade. Personuppgifterna kan komma från publika källor eller vara köpta från företag, och sammanställs för att skapa konsumentprofiler som säljs vidare. En sådan konsumentprofil kan till exempel innehålla data från mobiltelefoner som app-användning, annons-ID eller annan användaridentifiering och användarens kontakter. Personuppgifterna kan också omfatta webbrowser-användning, uppkopplade enheter och offentliga data. Det är ett stort antal olika företag som levererar data till olika datamäklare. Leverantörerna kan vara andra datamäklare, analysföretag, kreditkortsföretag och många andra företag. Det är inte alltid uppenbart var den insamlade informationen från andra tredjepartsaktörer initialt kommer ifrån.[218]

Information från spårningen av användare används sedan för att rikta de annonser som visas för användaren. Processen innebär att potentiella annonsörer kan se information om användarna, till exempel information om vilken enhet som används, vilken webbplats som besöks och vilket land användaren befinner sig i. Informationen kan också vara mer detaljerad, och inkludera tidigare besökta webbplatser, användarens intressen eller till exempel vilka hälsoproblem användaren sökt information om.

När en annons visas på en webbsida eller i en app, är det resultatet av en komplicerad budgivningsprocess i realtid (real-time-bidding, RTB), där hundratals annonsörer inom någon bråkdels sekund kan ha budat om att få visa sin annons. Själva auktionen kan ske på olika sätt; som en öppen auktion där många kan delta, mer slutna budgivningar eller genom överenskommelser med fast pris. Olika plattformar med olika tekniker för budgivning möjliggör processen.

216. Stefan Larsson Dataekonomier - *Om plattformar, tredjepartsaktörer och behovet av transparens på digitala marknader*, Konkurrensverket uppdragsforskning rapport 2020:4.

217. Stefan Larsson Dataekonomier - *Om plattformar, tredjepartsaktörer och behovet av transparens på digitala marknader*, Konkurrensverket uppdragsforskning rapport 2020:4.

218. Forbrukerradet *Out of control, How consumers are exploited by the online adversiting industry.*

5.4.3.2 Nyttor och risker med den digitala annonsindustrin

Hastigheten, omfattningen och komplexiteten i realtidsbudgivningen är tekniskt imponerande och underlättar försäljningen av annonsutrymme. Inkomster genereras till publicisterna och värde för annonsörerna. För den enskilde beskrivs ofta nyttan i termer av att vi får ett anpassat och mer relevant annonsutbud presenterat för oss.

I en studie finansierad av Handelsrådet som publicerades i december 2020 undersöks konsumenters inställning till hur handeln använder deras data, om rimligheten i utbytet och kunskapen om tredjeparters inblandning.[219] Trots det ofta framförda argumentet om att datainsamling och kundprofilering motiveras med att skapa relevanta reklamerbjudanden visar studien att en majoritet (57 procent) av konsumenterna inte tycker att det är rimligt att företag samlar in personlig information som motprestation för rabatterade varor och tjänster. Endast omkring 1 av 5 tycker att utbytet är rimligt, med något högre acceptans hos den yngre generationen. Stödet för identifiering via smartphone eller filmande i fysisk butik är särskilt svagt, där bara 1 av 10 tycker att det är rimligt i utbyte mot förmåner eller förbättringar av sina shopping-upplevelser. Datadelning till tredjepartsaktörer, det vill säga andra företag, ses som en av de känsligaste frågorna och på frågan om det är ok att företag delar kunders personliga information med andra företag svarade hela 4 av 5 "Nej, aldrig". Oroande för förtroendet för företag inom svensk handel är att närmare hälften (44 procent) saknar tilltro till att deras personuppgifter inte delas eller säljs vidare utan deras vetskap.

219. Larsson, Emanuelsson och Thiringer; *Tillit eller tvång? Konsumenters förtroende för handelns datainsamling.*

Ur ett användar- och medborgarperspektiv innebär den digitala annonsmarknaden och realtidsbudgivningarna stora risker för den personliga integriteten. Hela den digitala annonsindustrin bygger på en stark drivkraft att samla in så mycket uppgifter som möjligt, vilket normalt strider mot dataskyddsförordningens princip om uppgiftsminimering. Möjligheten att ta fram avancerade konsumentprofiler medför också en uppenbar risk för ändamålsglidning, det vill säga att personuppgifter används för andra ändamål än vad de ursprungligen samlats in för. Ett av de mest kända exemplen på ändamålsglidning är skandalen kring Cambridge Analytica. Ett annat exempel har rapporterats från Indien, där ett fintechbolag använde personuppgifter hämtade från musikappar som en del i sin kreditprövning. Kontaktlistor, user-ID och GPS-lokalisering inhämtades och användes för beslut om beviljande av lån. Medborgarna som sökte lån kände dock inte till att informationen användes, och kunde därmed varken protestera mot användningen eller invända mot besluten.[220]

Integritetsriskerna på den digitala annonsmarknaden bottnar i stor utsträckning i att större delen av den komplexa processen sker i det dolda och utan möjligheter till transparens för enskilda individer.[221] I användarvillkoren nämns tredjepartsaktörerna ofta inte vid namn, och även när namnen framgår, måste samtliga aktörers villkor läsas för att användarna ska förstå hur de samlar in och använder personuppgifterna. Användarvillkoren är dessutom svåra att förstå och i regel otillräckliga för att användarna ska kunna överblicka omfattningen av insamlingen, användningen och dess konsekvenser. Många gånger är det också krångligt att förstå vilka handgrepp eller inställningar som krävs för att neka insamling av personuppgifter. Sammantaget är det i praktiken omöjligt för medborgarna att få en överblick av hur deras personuppgifter används av tredjepartsaktörer.[222]

Ytterligare en integritetsrisk handlar om möjligheten att faktiskt identifiera enskilda individer i de stora datamängderna. Många företag hävdar att uppgifterna som samlas in är avidentifierade och inte kan kopplas till en individ. I realiteten går det dock ofta att identifiera enskilda individer via till exempel IP-adress eller user-ID. Dessutom innebär många olika uppgifter om en person att denne ofta går att identifiera.

220. https://www.huffingtonpost.in/entry/fintech-apps-privacy-snooping-credit-vidya_in_5d1cbc34e4b082e55373370a?guccounter=1.

221. Draft – Working Paper on *the Risks emerging from the Tracking and Targeting Ecosystem in the Digital Advertising Market*, International Working Group on Data Protection in Telecommunications, meeting 4-5 March 2020, Tel Aviv (Israel).

222. Forbrukerrådet *Out of control – How consumers are exploited by the online adversiting industry*,

Norska Forbrukerradet kom i rapporten *Out of Control* till slutsatsen att stora delar av den datadrivna reklambranschen systematiskt bryter mot dataskyddslagstiftningen (och därmed är illegal).[223] Även den brittiska dataskyddsmyndigheten ICO har, efter en ingående kartläggning och probleminventering med fokus på realtidsbudgivningar i den digitala annonsindustrin, kommunicerat en liknande slutsats.

Sammanfattningsvis pekar ICO ut tre områden där de bedömer att den digitala annonsindustrin på ett oroväckande sätt bryter mot dataskyddsförordningen.

Transparens

- Användarvillkor och personuppgiftspolicy är ofta otydliga och ger inte användarna full insyn i vad som händer med deras personuppgifter.
- De komplexa och icke transparenta processerna gör det svårt, eller i praktiken omöjligt, för den enskilde att utnyttja sina rättigheter, till exempel att få information raderad.
- Omfattningen av skapandet och delandet av konsumentprofiler är oproportionerlig, inkräktande och oriktig – särskilt som många användare är omedvetna om att processerna sker.

Rättslig grund – de flesta aktörerna i realtidsbudgivningar tycks enligt ICO:s kartläggning stödja sig på samtycke eller intresseavvägning som laglig grund. I många fall används även avtal som rättslig grund. ICO menar att en stor del av personuppgiftsbehandlingen är olaglig eftersom

- Avtal inte är lämpligt att använda som rättslig grund, givet det stora antalet involverade aktörer och karaktären på de personuppgifter som delas i realtidsbudgivningar.
- Samtycke sannolikt inte kan anses vara frivilligt och jämlikt, och därför inte är en giltig rättslig grund.
- Det är inte ovanligt att personuppgiftsbehandlingen inkluderar även känsliga personuppgifter, vilket enligt dataskyddsförordningen bara får ske i vissa undantagsfall. Ett sådant undantag kan vara att den enskilde uttryckligen lämnat sitt samtycke. Sannolikt är det svårt för den enskilde individen att överblicka vad ett sådant samtycke innebär.

Säkerhet – en realtidsbudgivning kan, inom någon bråkdels sekund, inkludera dussintals eller till och med hundratals aktörer. ICO:s kartläggning visar att

- Komplexiteten och de många aktörerna gör det svårt även för verksamheterna själva att fullt ut överblicka vem som tar del av vilken data. Att säkerställa tillräckliga säkerhetsåtgärder är därmed problematiskt.
- Konsekvensbedömningar saknas. Realtidsbudgivningar inkluderar ofta den typ av personuppgiftsbehandling som gör att det enligt dataskyddsförordningen finns krav på att genomföra en konsekvensbedömning. Många aktörer inom den digitala annonsindustrin tycks enligt ICO dock varken känna till eller förstå kraven på konsekvensbedömningar.

ICO menar att problemen i den digitala annonsindustrin genomsyrar hela branschen och kräver kraftfulla initiativ och självsanering i branschen för att lösas. Brittiska aktörer har också påbörjat flera förbättringsåtgärder med utgångspunkt i ICO:s probleminventering, bland annat har en branschorganisation för digital marknadsföring utarbetat en vägledning och tagit fram utbildningar på området. ICO är positiva till dessa åtgärder, men konstaterar samtidigt att arbetet hittills inte varit tillräckligt för att komma till rätta med problemen. Den brittiska dataskyddsmyndigheten bedömer därför att en ökad reglering, antingen i form av lagstiftning eller föreskrifter, i kombination med en skärpt tillsynsverksamhet behövs som ett nästa steg.

Sammanfattningsvis har tekniker för att bearbeta och använda stora datamängder utvecklats i lika stor utsträckning som teknik för att samla in data. Användningen av AI är avgörande för att kunna utvinna värde ur stora mängder data. Med allt mer komplexa och icke transparenta processer försvåras dock den enskilde individens förutsättningar att utöva sina rättigheter och kontrollera vem som använder ens data och för vilka syften.

223. Forbrukerradet Out of control – *How consumers are exploited by the online advertising industry*

5.5 Teknik för att lagra data

I takt med att insamling och bearbetning av data blir allt mer omfattande och sofistikerad växer också kraven på lagringskapacitet. Inom de flesta samhällsområden finns ett starkt behov av billig, snabb och anpassningsbar lagring, med kapacitet att hantera stora mängder data.

Den teknik som hittills svarat väl mot de stora behoven av lagringskapacitet är avancerad *molnlagring*. En utmaning med bearbetning eller lagring i molntjänster är att marknaden för molntjänster domineras av amerikanska aktörer, vilket kan medföra att lagringen efter EU-domstolens avgörande i juli 2020 i det så kallade Schrems II-ärendet inte är laglig.

Även utvecklingen inom IoT kräver ny lagringsteknik, som ger möjlighet till lagring, säkring och bearbetning direkt i enheterna utan att behöva transportera data i nätet. Sådan lagring benämns ofta *edge storage*.

I takt med att insamlingen och bearbetningen av data blir allt mer omfattande och sofistikerad växer också kraven på lagringskapaciteten. Inom de flesta samhällsområden finns ett starkt behov av billig, snabb och anpassningsbar lagring, med kapacitet att hantera mycket stora mängder data.

Ny lagringsteknik är exempelvis en förutsättning för utvecklingen inom AI-området, eftersom AI ofta kräver att omfattande datamängder i blandade format måste kunna lagras och hämtas mycket snabbt. Detta kräver hög kapacitet och prestanda i lagringslösningarna.

Även utvecklingen inom IoT kräver ny lagringsteknik, som ger möjlighet till lagring, säkring och bearbetning direkt i enheterna utan att behöva transportera data i nätet.

5.5.1 Molnifiering av lagring

Den teknik som hittills svarat väl mot de stora behoven av lagringskapacitet är avancerad molnlagring. ”Molnifiering” av lagring innebär att personuppgifter och annan data flyttas över till molnlösningar med stor lagringskapacitet som gör det möjligt för användarna att enkelt dela data mellan flera enheter. Inom molnlösningar sker också teknisk utveckling för att passa användarnas olika behov av säkerhet, kontroll och kapacitet. Ett fåtal globala aktörer kontrollerar idag en stor andel av marknaden.

Molntjänster är förenklat ett stort antal sammankopplade servrar som gentemot användarna fungerar som en enhet. Användarna vet att de lagrar sina data i ett ”moln”, men de vet sällan var i molnet eller på vilka servrar de finns, och behöver för funktionen vanligen inte veta det. Filerna kan flyttas om i molnet utan att det påverkar användarens tillgång till dem. Man kan säga att användaren bara behöver veta resursens namn, inte dess adress. Servrarna i ett moln kan vara spridda över ett större område, kanske i flera länder. Moln av servrar används för att sköta internetbaserade program och för att lagra stora datamängder. Tekniken ger möjlighet att tilldela resurskrävande program den kapacitet som behövs vid varje tidpunkt.[224] ”Multi-cloud” innebär att användaren utnyttjar flera parallella molnlösningar för olika datamängder, användningsområden och behov. ”Hybrid cloud” innebär molnlösningar där användaren blandar molnteknik som denne själv kontrollerar med molnteknik som kontrolleras av någon annan.[225]

En av drivkrafterna inom området är den växande insamlingen av data i kapacitetskrävande format, som exempelvis rörlig bild och ljud, samt användarnas önskemål att komma åt och kunna bearbeta all insamlad data överallt och närsomhelst.

Molnifieringen av lagring har också en koppling till utvecklingen inom digitalt samarbete, som omfattar verktyg, system och plattformar som syftar till att underlätta samarbeten, både lokalt och på distans. Digitala funktioner som delade dokumentarkiv och videokonferenser har fått ett stort genomslag i samband med att Covid19-pandemin ökat hemarbetet väsentligt.

224. https://it-ord.idg.se/ord/moln/.
225. https://www.omg.org/cloud/deliverables/CSCC-Practical-Guide-to-Cloud-Management-Platforms.pdf.

Molnifieringen väcker integritetsrelaterade frågeställningar kring bland annat ansvarsfördelning och vem som har tillgång till lagrade personuppgifter, i de fall uppgifterna lagras i molntjänst som kontrolleras av en tredje part. Offentlig sektor har särskilda utmaningar om sekretessbelagt material behandlas av en aktör som inte omfattas av sekretess. Uppgifterna får då ett svagare skydd om den som driftar tjänsten kan ta del av uppgifterna i klartext.[226]

En utmaning med bearbetning eller lagring i molntjänster är att dessa tjänster inte sällan är globala. För att få överföra personuppgifter till länder utanför EU krävs att det är tillåtet enligt dataskyddsförordningens regler om tredjelandsöverföring. Det är en utmaning för den personuppgiftsansvarige att i användning av molntjänster ha kontroll både på om personuppgifter överförs till tredje land och om det i så fall är tillåtet. Marknaden för molntjänster har, i vart fall hittills, dominerats av amerikanska aktörer, vilket kan medföra att lagringen efter EU-domstolens avgörande i det så kallade Schrems II-ärendet inte längre är laglig.[227] Domstolen slog i ärendet fast att kommissionens så kallade Privacy Shield-beslut om överföring av personuppgifter från EU till USA är ogiltigt efter som det inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till USA. Privacy Shield är en mekanism för självcertifiering som finns i USA. Den innebär att företag i USA kan anmäla sig till det amerikanska handelsdepartementet och meddela att de uppfyller de krav som ställs i Privacy Shield. Det har tidigare varit tillåtet för personuppgiftsansvariga i EU att överföra personuppgifter till amerikanska företag som har anslutit sig till Privacy Shield. EU-domstolens ogiltigförklarandet av Privacy Shield innebär att det inte längre är tillåtet för personuppgiftsansvariga i EU att med Privacy Shield som grund överföra personuppgifter till mottagare i USA.

226. Försök att komma tillrätta med detta behandlas i den tidigare nämnda propositionen, prop. 2019/20:201 om tystnadsplikt vid utkontraktering.

227. Dom av den 16 juli 2020, Facebook Ireland och Schrems, C-311/18, EU:C:2020:559.

5.5.2 Edge storage och nya lagringsmedia

Precis som behandling av data kan ske direkt i olika lokala enheter, genom edge computing, kan även lagring av data ske lokalt. Istället för att lagra all data centralt i nätverket kan data lagras lokal i till exempel en IoT-enhet. Sådan lagring benämns vanligen edge storage.

Nya lagringsmedia och ökad prestanda på lagringstekniken möjliggör snabbare, flexiblare och säkrare lagring. Utveckling sker bland annat inom flashminnen[228] och fiberteknik, samt anpassning av lagringslösningar för att passa AI-tillämpningar som kräver mycket stor kapacitet.[229]

Utvecklingen påverkar bland annat var personuppgifter lagras och förutsättningarna att spåra och förstöra lagrad data, vilket innebär att den även kan påverka den personliga integriteten.

5.5.2.1 Nyttor med nya lagringslösningar

I detta avsnitt ges kortfattade exempel på konkreta användningsområden för molnlagring och edge storage inom olika sektorer, som ger en bild över olika tillämpningsområden och potentialen med utvecklingen inom olika sektorer.

Bank, finans och försäkring – avancerade molnlösningar gör det möjligt att dra nytta av den stora mängd personuppgifter som företagen samlar in och att snabbt utveckla och implementera nya tjänster som kan användas både av företagens egen personal och i kundernas stationära och mobila enheter.[230]

Tillverkande industri – molnlösningar används för att hantera de stora datamängder från flera olika datakällor som krävs för att bland annat automatisera produktionsprocesser.[231] Ny lagringsteknik används också för industriella AI-applikationer i krävande miljöer, där tekniken måste fungera tillförlitligt trots föroreningar, stora temperaturskillnader och vibrationer.

228. Ett flashminne är en typ av minne som bevarar lagrade data när strömtillförseln stängs av. Flashminne används som alternativ till en hårddisk i till exempel musikspelare, bärbara datorer, mobiltelefoner, USB-minnen och annan bärbar utrustning. https://it-ord.idg.se/ord/flashminne/

229. https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/corporate/ieee-industry-advisory-board/digital-storage-memory-technology.pdf.

230. https://www2.deloitte.com/global/en/pages/financial-services/articles/bank-2030-financial-services-cloud.html.

231. https://www.startus-insights.com/innovators-guide/industry-4-0-innovation-map-reveals-emerging-technologies-startups/.

Handel – stora volymer av kunddata lagras och behandlas i molnlösningar. Molnlösningar för att lagra personuppgifter och annan data gör det möjligt för handlarna att hantera verksamhetskritiska funktioner såsom prissättning, individanpassad marknadsföring, lojalitetsprogram, lagerhantering och koordinering mellan försäljningskanaler i realtid och på ett mer resurseffektivt sätt.[232] Handlare kan även använda edge storage i form av övervakningskameror som tillfälligt lagrar data direkt i kameraenheterna, vilket bland annat medför att bevakningen fungerar även om nätet inte gör det.[233]

Hälso- och sjukvård – molnlösningar används för att lagra patientdata och enkelt dela den mellan sjukhus, apotek och andra aktörer som patienten kommer i kontakt med. Molnlösningarna gör det möjligt för aktörerna att hantera lagringen av stora mängder personuppgifter i patientjornaler, patientportaler, mobilapplikationer och liknande på ett koordinerat, skalbart och kostnadseffektivt sätt.[234] Med edge storage kan nya medicinska enheter både samla in och bearbeta patientdata i realtid, utan behov att skicka och hämta data från centraliserade datacenter.[235]

Media – ny lagringsteknik används bland annat för att hantera strömmande media i resurskrävande format, som ska kunna distribueras till många mottagare samtidigt. Lätt skalbara molntjänster används också för att hantera svängningar i belastning på exempelvis beställvideotjänster.[236]

Transporter – molnbaserade tjänster och plattformar används i bilar och andra fordon.[237]

Användningen av molntjänster påverkar den personliga integriteten på flera sätt; det handlar om vilka personuppgifter som lagras, hur och var de lagras, hur många olika ställen som uppgifterna lagras på samtidigt och vem eller vilka som kontrollerar lagringen och har åtkomst till uppgifterna. En mer lokal lagring kan innebära ett förstärkt integritetsskydd, men förutsätter samtidigt att säkerheten i den lokala enheten är god.

5.6 Teknik för att transportera data

En ökad insamling och förmåga att bearbeta och använda data ställer också helt nya krav på infrastruktur och teknik för att transportera stora datamängder.

5G är nästa generation av mobila nätverk med extremt hög kapacitet för att transportera data. Ett centralt användningsområde för 5G kommer att vara IoT med till exempel uppkopplade enheter i industrin och i smarta städer. En integritetsrisk kopplat till 5G handlar om att geografisk positionering kommer vara möjligt med mycket större precision än idag.

Andra former av *digital kommunikationsteknik* som nu utvecklas tar sikte på kommunikation på nära avstånd, till exempel mellan enheter i ett och samma rum eller i chip som kan monteras i prislappar.

Personlig data som samlats in transporteras ofta många gånger mellan olika enheter och användare inom en verksamhet. Det kan vara frågan om verksamheter som inte har data och analysresurser samlade på en enda plattform och som behöver överföras till en annan plattform. Det kan också vara frågan om att man behöver kombinera data från olika källor på ett effektivare sätt. Därför finns ett behov av att kunna transportera data på ett snabbt och säkert sätt.

Data transporteras också mellan olika verksamheter. Tidigare har transport bland annat kunnat ske genom olika former av lagringsmedium, såsom disketter, USB-minnen eller externa hårddiskar. Idag bidrar internet och molnifieringen till att möjliggöra nya former av transport i olika dataflöden.

232. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-cloud-as-catalyst-for-retail.
233. https://www.axis.com/sv-se/technologies/edge-storage.
234. https://www.healthitoutcomes.com/doc/where-should-healthcare-data-be-stored-in-and-beyond-0001.
235. https://www.vxchnge.com/blog/edge-computing-use-cases.
236. https://www.startus-insights.com/innovators-guide/entertainment-innovation-map-reveals-emerging-technologies-startups/.
237. https://www.ericsson.com/en/cases/2017/partnerships-built-on-innovation.

Den parallella utvecklingen med bland annat allt fler konsumentprodukter och tjänster som är mobila, AI, avancerade molntjänster och IoT ställer också helt nya krav på teknisk infrastruktur och teknik för att transportera stora datamängder. Personuppgifter som samlas in ska vara tillgängliga närsomhelst och varsomhelst, utan väntetider eller fördröjning.[238]

Digital kommunikationsteknik utvecklas för att möta dessa krav och den nya tekniken innebär både möjligheter och nya risker för integritetsskyddet.

5.6.1 5G

5G är nästa generation av mobila nätverk med extremt hög kapacitet för att transportera data. En företrädare för telekom-branschen beskriver att ”5G kommer att ge oss det uppkopplade samhället på riktigt. En värld där det digitala och fysiska flyter samman, med nästintill oändliga möjligheter att koppla upp och koppla ihop saker, företag och samhällsfunktioner”.[239]

5G innebär möjligheter som snabbare uppkoppling och möjlighet att hantera stora mängder data. Internationella forskare lyfter samtidigt fram risker, till exempel när det gäller nationell säkerhet och personlig integritet.[240]

Det har sedan 2018 funnits 5G-nät för forskning och utveckling, men först i slutet av maj 2020 startades Sveriges första publika kommersiella 5G-nät. I Sverige har myndigheten Post- och telestyrelsen (PTS) ett samlat ansvar för elektronisk kommunikation, vilket bland annat innebär att främja tillgången till säkra och effektiva elektroniska kommunikationer.[241] Auktionen av 5G-frekvenser har försenats efter att PTS beslut om att utesluta det kinesiska företaget Huawei från auktionen överklagats. Beslutet baseras på ett samrådsyttrande från Säkerhetspolisen och Försvarsmakten där Kina pekas ut som ett av de största hoten mot Sverige. Säkerhetspolisen konstaterar att den kinesiska staten bedriver omfattande cyberspionage för att främja sin egen ekonomiska utveckling och utveckla sin militära förmåga – ett faktum som Sverige behöver förhålla sig till när 5G-nätet byggs.[242]

5G är inte i första hand avsedd för röstsamtal, utan för snabb, mobil dataöverföring med hög bandbredd. Ett stort användningsområde kommer att vara IoT i industri och smarta städer, där det är tätt mellan terminaler som kommunicerar mobilt. 5G är utformat för att terminalerna ska kunna vara påslagna ständigt med minimal strömförbrukning när de inte används.

Tekniken innebär högre hastigheter, mindre fördröjning och ökad (drift)säkerhet, vilket är speciellt viktigt för industriella applikationer. En likhet med tidigare generationer av mobila nätverk är att nätverket hela tiden vet var en användare finns, förutsatt att användarens telefon (eller annan utrustning för mobil datakommunikation) är påslagen, men med mycket större precision än tidigare generationers mobila nätverk.[243] Samtidigt möjliggör 5G överföring av högupplösta bilder med mycket större precision och hastighet än tidigare nätverk. Möjligheten att med minskad fördröjning transportera bildmaterial lär, tillsammans med utveckling inom till exempel mjukvara för bildstabilisering, skapa mer möjligheter och incitament till insamling av biometrisk data från till exempel ansikten.

5.6.2 Digital kommunikationsteknik

Området för digital kommunikationsteknik innefattar bland annat teknik för mobil kommunikation (mobil infrastruktur, mobila nätverk, mobila standarder, mobila enheter och mobila tjänster), snabbare och bättre internet och teknik för digital kommunikation på korta avstånd, så kallad ”near field communication”.

Utvecklingen drivs i flera parallella spår och syftena är bland annat att uppnå snabbare och resurseffektivare kommunikation med bättre täckning.[244] Exempel på utvecklad teknik är följande.

- Li-Fi – en teknik för snabb dataöverföring genom belysningen i ett rum. Snabba och för människor omärkliga variationer i ljusstyrkan kodar ett dataflöde som kan uppfångas av sensorer i datorer, mobiltelefoner och annan elektronik.[245]
- LPWAN (low power wide area network) – trådlösa nätverk med låg strömförbrukning och lång räckvidd. Som ”lång räckvidd” räknas här ungefär en kilometer eller mer. Sådana nätverk är önskvärda för IoT, i synnerhet utomhus och på avstånd från bebyggelse och eluttag. Datamängderna som ska överföras i IoT är ofta små, så det behövs inte mycket bandbredd, vilket innebär låg strömförbrukning.[246]
- Fiberteknik med högre hastigheter och mindre fördröjning.
- Satellitkommunikation som möjliggör global täckning med mindre fördröjning än dagens satelliter.

238. http://events17.linuxfoundation.org/sites/events/files/slides/Keynote_Dr.%20Uddenfeldt.pdf.
239. www.telenor.se, citat från Kaaren Hilsen, VD Telenor Sverige.
240. Komet informerar 2020:30 *Den nya tekniken – så fungerar den*.
241. Komet informerar 2020:30 *Den nya tekniken – så fungerar den*.
242. https://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2020-10-20-sakert-5g-viktigt-for-sverige.html.

243. https://www.fastcompany.com/90314058/5g-means-youll-have-to-say-goodbye-to-your-location-privacy.
244. https://medium.com/@seanmoffitt/the-top-30-emerging-technologies-2018-2028-eca0dfb0f43c.
245. https://it-ord.idg.se/ord/li-fi/.
246. https://it-ord.idg.se/ord/low-power-wide-area-network/.

Teknikområdet påverkar förutsättningarna för utvecklingen inom IoT och edge computing, men också andra aktuella teknikområden såsom AI och molntjänster, vilka alla har en potentiellt stor inverkan såväl på tekniken som på den personliga integriteten.[247]

Utveckling sker också för att öka möjligheten till kommunikation på korta avstånd (proximity tech). Området innefattar bland annat radiofrekvensteknik som kan byggas in till exempel i prislappar, nya generationer av Bluetooth, WiFi som kan hantera högre hastigheter och fler uppkopplade enheter, närfältskommunikation som används till exempel i busskort och mobiltelefoner för betalning och så kallad geofencing. Det senare är virtuella "staket" baserade på exempelvis GPS-teknik och används för att avgränsa områden inom vilka dataöverföring sker. Inom transportsektorn är geofencing en digital geografisk zon där uppkopplade fordon kan styras på olika sätt, till exempel för att begränsa ett fordons tillgång till zoner.[248]

5.6.2.1 Exempel på konkreta användningsområden och berörda sektorer

I detta avsnitt ges kortfattade exempel på konkreta användningsområden för utvecklad teknik för transport av data inom olika sektorer, som ger en bild över olika tillämpningsområden och potentialen med utvecklingen inom olika sektorer.

Transport – låg fördröjning i dataöverföringen i de mobila näten är en avgörande förutsättning för självförande fordon, och de nya tjänster som bygger på kommunikation fordon-till-fordon och fordon- till- infrastruktur.[249]

Handel – med hjälp av proximity tech kan butiksägare samla in data om var kunderna befinner sig i butiken och kommunicera marknadsföringsbudskap och annan information direkt till deras smarta telefoner.[250]

Tillverkande industri – snabbare digital kommunikationsteknik möjliggör produktions- och underhållssystem som arbetar i realtid.[251]

Offentlig sektor – teknik för datakommunikation över långa avstånd gör det bland annat möjligt för myndigheter att säkra kommunikationsvägar mellan samhällsviktiga funktioner, i nätverk som staten själv kan kontrollera.[252]

Försvar – nya kommunikationsmöjligheter mellan system och plattformar möjliggör tekniskt avancerad strid med olika system i samverkan. Med snabb överföring av data kan olika förband integrera sensorer, ledningsfunktioner, vapenbärare och vapen.[253]

Hälso- och sjukvård – infrastruktur med hög driftsäkerhet och hög kapacitet för dataöverföring är en förutsättning för telemedicintjänster[254] och övervakning av patienter på distans.[255]

Energi – energisektorn har mycket infrastruktur som tidigare inte varit uppkopplad, av kostnadsskäl och för att infrastrukturen ofta är lokaliserad långt ifrån de befintliga kommunikationsnätverken, men som med hjälp av ny och utvecklad teknik nu kan kopplas upp.[256]

Media – sociala media och videotjänster där privatpersoner lägger upp ljud och rörlig bild, både inspelat och i realtid kräver en all större kapacitet i både de stationära och de mobila näten.

Forskning – teknik för datakommunikation över långa avstånd gör det bl.a. möjligt för forskare att bevaka seismisk aktivitet över stora geografiska områden i realtid.[257]

Sammanfattningsvis finns stora möjligheter med nya former för att transportera data. Eftersom tekniken bland annat används för att lokalisera och interagera med enskilda individer kan tekniken få påverkan även på den personliga integriteten.[258] I en värld där det digitala och det fysiska flyter samman genom alla möjligheter som enbart 5G kommer att ge i att koppla upp och ihop saker, verksamheter och funktioner, så påverkas även den personliga integriteten. Det är redan idag svårt att förstå vilka digitala avtryck man ger som individ. Komplexiteten och kapaciteten kommer med utvecklad teknik för att transportera data öka med en extrem hastighet. Detta för med sig att den enskilde inte kommer att ha någon möjlighet till överblick eller kontroll om inte verksamheterna från början bygger in transparens.

247. https://web.archive.org/web/20190406032845/https://business-institute.dk/media/2984/the-wiki-brands-trend-collection.pdf sid.19.

248. https://www.trafikverket.se/resa-och-trafik/forskning-och-innovation/aktuell-forskning/transport-pa-vag/geofencing/.

249. https://www.zdnet.com/article/five-industries-that-will-be-most-affected-by-5g/.

250. https://risnews.com/five-things-retailers-should-know-about-proximity-solutions.

251. https://www.zdnet.com/article/five-industries-that-will-be-most-affected-by-5g/.

252. https://en.wikipedia.org/wiki/Long-range_Wi-Fi#Nonprofit_and_Government.

253. https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/perspektivplan/slutlig-redovisning-av-perspektivstudien-2016-2018.pdf.

254. Telemedicin är en sammanfattande term på olika tillämpningar inom sjukvården där telekommunikation används för att överföra icke-verbal medicinsk information. https://www.medicinskordbok.se/term/telemedicin/.

255. https://www.zdnet.com/article/five-industries-that-will-be-most-affected-by-5g/.

256. https://www.zdnet.com/article/five-industries-that-will-be-most-affected-by-5g/.

257. https://en.wikipedia.org/wiki/Long-range_Wi-Fi#Nonprofit_and_Government.

258. https://www.lexology.com/library/detail.aspx?g=24f71dc6-c0c7-444e-92d2-8f013bf08f9e.

5.7 Teknik för att säkra data

Att säkerställa tillräcklig säkerhet för personuppgifter omfattar alla aspekter av informationssäkerhet, det vill säga både tekniska och organisatoriska säkerhetsåtgärder men även inbyggt dataskydd genom privacy by default och by design.

Utvecklingen med fler uppkopplade enheter och ökad molnlagring har ökat antalet möjliga vägar för angripare att komma åt system, nät, datorer, enheter eller servrar. En ökad hotbild har drivit på utvecklingen av ny *säkerhetsteknik* som till exempel automatiserade säkerhetslösningar baserade på AI.

Edge computing för också med sig krav på teknik för *edge security*, det vill säga att personuppgifter kan säkras direkt i de lokala enheter där de samlas in – exempelvis i en privatpersons smarta mobiltelefoner.

Nya och fler lättanvända *krypteringslösningar* har också utvecklats de senaste åren.

Ytterligare ett område under utveckling är *blockkedjor*, som kan användas för att lagra och säkra information. Blockkedjor rymmer, precis som viss annan säkerhetsteknik, både möjligheter och utmaningar ur ett dataskyddsperspektiv.

Rätt använd kan den nya tekniken stärka integritetsskyddet.

För att säkerställa att insamling, bearbetning, lagring och transport av data får genomföras och också genomförs på ett sätt som uppfyller lagstiftningens krav behöver data säkras. Säkerheten för data är central under hela livscykeln och går sällan att säkerställa om den inte byggs in och beaktas från början.

Att säkerställa tillräcklig säkerhet för personuppgifter omfattar alla aspekter av informationssäkerhet – det vill säga säkerhetsåtgärder för att bevara konfidentialitet, riktighet och tillgänglighet för uppgifter i både fysisk och digital form. Arbetet innefattar både tekniska säkerhetsåtgärder och administrativa eller organisatoriska säkerhetsåtgärder,[259] men även inbyggt dataskydd genom privacy by default och by design.[260] Även om olika säkerhetsåtgärder delvis har olika perspektiv finns också gemensamma nämnare och beröringspunkter som gör att åtgärder inom ett delområde, direkt eller indirekt, ofta leder till höjd säkerhet inom de andra områdena.

Den sammanlagda teknikutvecklingen med bland annat användningen av sensorer och sändare, IoT, webbskrapningstekniker och AI har medfört ökade krav på utvecklingen av digitala säkerhetslösningar. I takt med att allt fler verksamheter flyttar både data och applikationer till molnet och digitaliserar sina processer ökar också antalet vägar som finns för angripare att komma åt system, nät, datorer, enheter eller servrar.[261] När antalet möjliga säkerhetshot växer ökar behovet av att automatisera säkerhetsskyddet och att göra det mer ”intelligent”. Detta driver fram nya tekniska lösningar även inom säkerhetsområdet. Även införandet av en dataskyddslagstiftning med skarpare sanktionsmöjligheter har drivit på en allt snabbare utveckling inom säkerhetsområdet.

Nya tekniska lösningar ökar privatpersoners möjligheter att skydda sina personuppgifter och ger också verksamheter bättre förutsättningar att säkra känsliga data som samlas in. Samtidigt utvecklas hela tiden metoder för att hacka eller komma åt data med bristande säkerhet.

En stor utmaning inom säkerhetsområdet är att antagonistiska aktörer med skadliga intressen (till exempel enskilda hackers, organiserad brottslighet och främmande makt) i stor utsträckning har tillgång till samma teknik som de ”nyttiga” intressenterna. AI används till exempel av hackers för att bland annat identifiera säkerhetsbrister. Ny krypteringsteknik används för att kryptera skadlig kod, som därmed blir svårare för säkerhetsexperter att hantera.[262]

259. SIS-TR 50:2015 *Terminologi för informationssäkerhet*.

260. Artikel 25 dataskyddsförordningen.

261. https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx sid. 50.

262. https://www.techradar.com/news/encryption-2020s-double-edged-sword.

5.7.1 AI-baserad säkerhetsteknik och edge security

Inom flera av de teknikområden som beskrivits tidigare har utvecklingen också bidragit till nya typer av säkerhetslösningar. Ett exempel är automatiserade säkerhetslösningar baserade på AI. Tekniken gör det möjligt för säkerhetsansvariga att bevaka och skydda större system med många potentiella säkerhetsluckor och den kan förebygga och upptäcka säkerhetsbrister på alla nivåer, i nätverk, applikationer, operativsystem, hårdvara, system etcetera.[263]

Exempel på delområden där det utvecklas ny säkerhetsteknik baserad på AI är:[264]

- **Bedrägeriprevention och identitetskontroll** – för att säkra transaktioner, förhindra bedrägerier och identifiera bedragare med hjälp av maskininlärning.
- **Mobil säkerhet** – för att exempelvis identifiera skadlig kod i mobilapplikationer.
- **Beteendeanalys och prediktiv intelligens** – som lärt sig att upptäcka avvikelser i en verksamhets system och nätverk som kan vara tidiga tecken på en cyberattack.
- **Automatiserad säkerhet** – som bland annat innebär en automatisering av arbetsuppgifter som tidigare utfördes av säkerhetsexperter.
- **App-säkerhet** – AI-stöd till utvecklare av applikationer och analys av enskilda applikationer.
- **”Vilseledande säkerhet”** – AI-program som förebygger och avbryter pågående cyberattacker genom att vilseleda attackerarna, exempelvis genom att skapa stora neurala nätverk av fejkade datorer, enheter och tjänster.

AI innebär risker för ökad övervakning och en inskränkning av den personliga integriteten. Rätt använd kan AI-baserad säkerhetsteknik stärka integritetsskyddet.

Nya användningsområden för gammal teknik, exempelvis mobila nätverk, har de senaste åren skapat större fokus på säkerhet även på teknikområden som tidigare lämnats förhållandevis öppna och osäkra, till exempel IoT, där många produkter tidigare visat sig ha bristande säkerhet.

Edge computing och edge storage för också med sig krav på edge security, det vill säga att personuppgifter kan säkras direkt i de enheter där de samlas in. I bästa fall kan edge security innebära att de registrerade får ökad kontroll över sina egna personuppgifter.[265]

263. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf.

264. https://www.cbinsights.com/research/cybersecurity-artificial-intelligence-startups-market-map/.

265. https://edge.app/blog/edge-security-a-new-paradigm-in-privacy-and-security/.

5.7.2 Krypteringsteknik

Ny krypteringsteknik och ökad prestanda för befintlig krypteringsteknik utvecklas kontinuerligt. Tekniker för pseudonymisering och kryptering anges också i dataskyddsförordningen som exempel på säkerhetsåtgärder som bör övervägas för att säkerställa skyddet för personuppgifter.[266]

Krypteringslösningar kan användas både av verksamheterna som samlar in och lagrar personuppgifter, men också av enskilda individer.[267] Nya och fler lättanvända krypteringslösningar har utvecklats de senaste åren. Det bedöms underlätta förutsägbarheten och ge ökad kontroll över vem som har tillgång till vilka uppgifter och vem som är avsändare och mottagare för vissa uppgifter.

När det gäller säkerhetslösningar kan, som tidigare nämnts, den nya tekniken också utnyttjas för att åstadkomma skada, exempelvis utpressningsattacker. En förutsättning är ofta att hotaktörer ligger steget före och utnyttjar sin kunskap om teknikutvecklingen för att hitta svagheter i befintliga säkerhetslösningar.

Kvantdatorer med mycket större beräkningskraft än dagens superdatorer, anses av vissa bedömare kunna sätta många av dagens ”säkra” krypteringsalgoritmer ur spel. Teknikområdet innefattar därför även det som kallas ”post-quantum cryptography”, vilket innebär utveckling av kryptografiska algoritmer som ska kunna stå emot attacker med de kvantdatorer som nu utvecklas.[268] En kvantdator kan lösa komplexa problem mycket snabbare än en vanlig dator. En beräkning som skulle ta flera år kan istället göras på några sekunder. Utvecklingen av kvantdatorer är i en tidig utvecklingsfas, men har lockat till sig resursstarka investerare i form av både statliga aktörer och globala tech-företag. Såväl inom EU som i svensk forskning har kvantdatorer hög prioritet. Kompletta system för kvantberäkningar, särskilt sådana som är kommersiellt hållbara, ligger dock troligtvis decennier bort. Omfattande utmaningar handlar till exempel om att skala upp systemen, att utveckla kontrollsystem, att få stabila system och att undvika störningar från omgivningen, att skapa metoder för effektiv transformering av stora mängder data i ”klassiskt format” samt att designa algoritmer och utveckla mjukvara.[269]

266. Artikel 32.1 (a) dataskyddsförordningen.

267. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786244/HO_OSCT_Future_Tech_Trends_Final_Updated_13Mar19.pdf.

268. https://en.wikipedia.org/wiki/Post-quantum_cryptography.

269. Komet informerar 2020:30 *Den nya tekniken – så fungerar den.*

5.7.3 Teknik baserad på blockkedjor

Blockkedjor kan beskrivas som teknik som används för att säkra och öka kontrollen över information, det kan till exempel handla om olika lösningar för identifiering, ökad spårbarhet och minskad risk för manipulering. En viktig funktion av tekniken är att kunna minska antalet mellanhänder i en leverantörskedja och därmed minska risken för felkällor.

Idag förknippas tekniken i första hand med bitcoin och andra kryptovalutor, men andra användningsområden utvecklas i snabb takt, både inom privat och offentlig sektor.

Förenklat kan en blockkedja beskrivas som en distribuerad lista (en liggare), uppdelad i block, över transaktioner som berör ett digitalt objekt. Att listan är distribuerad innebär att den finns i identiska exemplar på många datorer. Att den kallas för kedja beror på att den är indelad i block, där varje nytt block sammanlänkas och innehåller ett kondensat (hash) av det föregående blocket. En jämförelse kan göras med sidorna i en kassabok, där varje ny sida börjar med summan av transaktionerna på den föregående. I en blockkedja är matematiken mer avancerad. Varje dator signerar med sin elektroniska signatur. Syftet är att det ska vara omöjligt att förfalska informationen då varje ny transaktion måste godkännas av ett antal datorer i blockkedjans nätverk. Dessa datorer har redan blockkedjan med alla tidigare transaktioner, och kan därför kontrollera att inga värden har ändrats sedan sist. De kan också kontrollera att den som gör transaktionen har rätt att göra det. Om allt stämmer godkänner de transaktionen och lägger den till listan (det aktuella blocket). Som regel krypteras alla transaktioner, blockkedjan lagras i krypterad form och det finns inte någon central server.[270]

Ur perspektivet personlig integritet innebär tekniken och de nya användningsområdena både möjligheter och utmaningar. Möjligheter som lyfts fram av internationella forskare handlar bland annat om datasäkerhet, möjligheten att verifiera att data inte har manipulerats, transparens samt bred tillgänglighet.[271]

Personuppgifter som hanteras med blockkedjeteknik kan exempelvis vara svårare att komma åt för hotaktörer, då all data inte är samlad på en central server. För att manipulera data i en blockkedja behöver man göra intrång i flera datorer i nätverket och dessutom forcera krypteringen. Den inbyggda spårbarheten kan också medföra att det blir både enklare och säkrare att hantera medgivanden när personuppgifter ska hanteras av flera olika aktörer och i olika syften. Tekniken kan också möjliggöra effektivare arbetsflöden både för verksamheter och för deras slutanvändare.[272]

Samtidigt finns en rad dataskyddsutmaningar med blockkedjeteknik. En central fråga rör hur dataskyddsförordningens grundläggande principer om uppgiftsminimering och rättslig grund kan kombineras med en teknik som är konstruerad för att information ska finnas för alltid och vara utspridd. Andra utmaningar handlar till exempel om hur rätten att bli bortglömd ska hanteras i en blockkedja där data lagras i samtliga datorer i blockkedjans nätverk, vem som är personuppgiftsansvarig i ett system där data är distribuerad i ett stort nätverk med många datorer och hur kontroll av tredjelandsöverföringar av personuppgifter i en publik blockkedja, där alla datorer i nätverket kan komma åt aktuella data, kan genomföras.

Det finns också andra rättsliga utmaningar, som till exempel i vilken mån så kallade smarta kontrakt som bygger på blockkedjor svarar mot traditionell lagstiftning. Ett smart kontrakt är ett kontrakt i form av ett datorprogram som verkställer åtagandena i kontraktet och som är baserat på en blockkedja. Parterna undertecknar kontraktet med elektroniska signaturer, och varje åtgärd som det smarta kontraktet sedan vidtar måste godkännas av ett antal parter i blockkedjans nätverk.[273]

Andra utmaningar rör skalbarhet, hållbarhetsaspekter (då tekniken kräver mycket el), att det är oklart hur säkerheten ser ut på längre sikt samt risken att blockkedjor missbrukas av totalitära regimer.[274] Just nu pågår ett intensivt arbete bland både privata och statliga aktörer för att finna lämpliga lösningar på dessa, och andra, regulatoriska och tekniska utmaningar med blockkedjetekniken.

270. https://it-ord.idg.se/ord/blockkedja/.
271. Komet informerar 2020:30 *Den nya tekniken – så fungerar den.*

272. https://iapp.org/media/pdf/resource_center/blockchain_and_gdpr.pdf.
273. https://it-ord.idg.se/ord/smart-kontrakt/.
274. Komet informerar 2020:30 *Den nya tekniken – så fungerar den.*

Nedan ges kortfattade exempel på konkreta utvecklings- och användningsområden för blockkedjeteknik:

- Applikationer för att möjliggöra enklare, snabbare och säkrare finansiella transaktioner. tekniken utvecklas av centralbanker, privata banker och andra aktörer. Den svenska Riksbanken driver till exempel ett pilotprojekt som undersöker teknik för en digital centralbankspeng, en e-krona. Den tekniska lösningen kommer att baseras på den teknik som används i blockkedjor.[275] Ett annat aktuellt delområde inom finansområdet kallas ”decentraliserad finans”, vilket innebär en form av finansiering som inte är beroende av centrala finansiella mellanhänder som mäklare, börser eller banker, utan istället använder smarta kontrakt på blockkedjor.
- Regeringen har gett Lantmäteriet och Myndigheten för digital förvaltning, DIGG, i uppdrag att testa ny teknik för automatisering i den offentliga förvaltningen. Inom ramen för uppdraget ska myndigheterna testa om blockkedjeteknik kan vara ett sätt att öka transparensen. Lantmäteriet har tillsammans med bland annat Skatteverket drivit ett utvecklingsprojekt som vunnit internationell uppmärksamhet. Projektet genomfördes 2018 och innefattade världens första helt digitala fastighetsöverlåtelse med hjälp av en blockkedjelösning.[276]
- Inom hälso-och sjukvårdssektorn utvecklas bland annat applikationer för säker hantering av patientjournaler och annan känslig information, där det krävs en hög säkerhet kring vem som kan komma åt känsliga personuppgifter. Den information som delas är inte ursprungsdokumenten, som till exempel register och patientjournaler, utan verifikationer av dessa.[277]
- Inom området logistik och försörjningskedjor används blockkedjeteknik bland annat för att reducera antalet mellanhänder och riskerna för misstag. I en blockkedja, med dess distribuerade liggare, kontrolleras att data som delas av alla parter i nätverket är korrekt – automatiskt och i alla steg.[278]
- Inom media och underhållning används blockkedjeteknik bland annat för förenklad hantering av upphovsrättigheter och närliggande rättigheter. Blockkedjebaserad teknik gör det möjligt för artisterna att på ett mer transparent sätt följa streamingföretagens användning av rättighetsskyddat material, vilket gör det möjligt för artisterna att kräva en rättvis ersättning.[279]

Sammanfattningsvis rymmer blockkedjor och annan teknik som kan förbättra säkerheten både möjligheter och utmaningar. Ofta gynnas dataskyddet av en förstärkt informationssäkerhet, men som blockkedjetekniken visar kan det också finnas motsättningar mellan en ökad säkerhet och ett gott dataskydd, som också innefattar krav bland annat på transparens och information.

275. Komet informerar 2020:30 *Den nya tekniken – så fungerar den.*

276. https://www.lantmateriet.se/contentassets/8d2b5d7647634c02a-329b01e46e61071/publikation-swe-fastighetskop-och-lagfart-ge-nom-en-blockkedja--governance-och-juridik-2018.pdf.

277. http://www.pharma-industry.se/blockkedjan/.

278. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641544/EPRS_STU(2020)641544_EN.pdf sid.10-11.

279. https://feminvest.se/2020/07/29/fokus-2020-kommer-att-ligga-pa-dessa-10-mojliga-anvandningar-for-blockchain/.

5.8 Teknik för att förstöra data

En konsekvens av att lagringskapaciteten har ökat och att kostnaderna för lagring har minskat är att incitamenten att förstöra data minskat. Tidigare förstördes gammal data ofta för att hushålla med lagringsutrymme och göra plats för ny.

Inom övriga områden har teknikutveckling inom ett område drivit på utvecklingen inom andra områden. När det gäller teknik för att förstöra av data har utvecklingen snarast gått i motsats riktning, och väsentligt större fokus har lagts på ny *teknik för att återskapa raderad data*, än teknik för att permanent förstöra den.

En konsekvens av att lagringskapaciteten har ökat och att kostnaderna för lagring har minskat är att incitamenten att förstöra data minskat. Tidigare förstördes gammal data ofta för att hushålla med lagringsutrymme och göra plats för ny.

Utvecklingen inom de övriga stegen i livscykeln har inte drivit på, och matchas inte heller av, en motsvarande utvecklingstakt av ny teknik och nya metoder för att förstöra personuppgifter.[280]

Tvärtom blir uppgiften att permanent förstöra – utplåna – personuppgifter allt svårare i takt med att uppgifter lagras på fler ställen som är geografiskt utspridda och kontrolleras av flera olika aktörer, kontinuerligt transporteras inom och utanför olika verksamheter via både trådlösa och fasta nät, och bearbetas med allt mer avancerad och mindre transparent teknik.

En annan faktor som försvårar möjligheterna att permanent förstöra data är utvecklingen av allt mer effektiv teknik för att återskapa raderad, eller på annat sätt förlorad, data. Även här finns, som beskrivits ovan när det gäller till exempel blockkedjor, alltså en potentiell motsättning mellan säkerhetsåtgärder och dataskydd. Även om innehållet på en hårddisk (det vanligaste mediet för datalagring) eller annat lagringsmedium har raderats eller skrivits över brukar det gå att rekonstruera innehållet med speciella metoder. Det krävs därför särskilda åtgärder för att utplåna det som har raderats från en hårddisk helt och göra det oläsbart. Även en fil som har skrivits över med en annan fil kan avläsas helt eller delvis. Vanlig radering av en fil på en disk innebär egentligen inte radering alls. Det innebär bara att filen stryks ur filkatalogen och det utrymme på hårddisken där den finns betraktas som ledigt. Filens innehåll (ettor och nollor) ligger ändå kvar tills det skrivs över av en annan fil, och det kan avläsas av program som bortser från filkatalogen.[281]

Överskrivning är en väl beprövad teknik som fortfarande används för att permanent förstöra data på en hårddisk eller annat lagringsmedium. Det sker vanligen genom att man skriver över datamängden med meningslösa sifferserier. Syftet är att de raderade tecknen ska bli omöjliga att urskilja, ens med specialverktyg. För att det ska bli omöjligt att rekonstruera filen krävs vanligtvis att överskrivning utförs flera gånger – vilket kräver tid och tar systemresurser i anspråk.[282] Det finns därför risk för att data som faktiskt ska raderas finns kvar över tid på ett sätt som dels inte uppfyller regelverkens krav på gallring, dels innebär ett ansvar för att säkerställa säkerheten för uppgifterna över tid.

Här förtjänar att nämnas att alla uppgifter inte får utplånas eftersom det inom offentlig verksamhet finns särskilda krav på bevarande, ibland över längre tid, ibland för evigt. Data ska då tas omhand för arkivering. Även för arkiverad data kvarstår ansvaret för att säkerställa säkerheten för uppgifterna över tid. Det ansvaret ökar i takt med teknikutvecklingen eftersom allt mer data idag lagras i elektroniska arkiv.

280. Det följer idag av principen om uppgiftsminimering i dataskyddsförordningen att data inte får sparas längre än nödvändigt.

281. https://it-ord.idg.se/ord/dataremanens/.
282. https://it-ord.idg.se/ord/overskrivning/.

5.8.1 Teknik för att återskapa raderad eller på annat sätt förlorad data

Relativt lite uppmärksamhet synes ges åt utvecklingen av nya och effektiva metoder att förstöra personuppgifter så att de inte kan återskapas igen. Desto mer uppmärksamhet får området ”computer forensics” som bland annat innefattar teknik för att återskapa raderade filer. Tekniken används exempelvis av polis och säkerhetstjänster för att återskapa raderad information i misstänkta personers datorer och mobiltelefoner och av privatpersoner som önskar rädda filer som raderats av misstag. Men den kan också användas av hackers för att återskapa och stjäla känslig information.

Nedan ges kortfattade exempel på konkreta utvecklings- och användningsområden för teknik för att återskapa data.[283]

- Återskapa raderad data från fysiska lagringsmedium som hårddiskar – exempelvis en raderad fil eller allt innehåll på en formaterad hårddisk.
- Återskapa raderad data från molnet – via buffertminne (minne som mellanlagrar sådant som ska användas inom kort).
- Analysera och extrahera data från en dators arbetsminne (det minne som innehåller aktiva program och de data som bearbetas när datorn används). Denna typ av minne töms vanligen på data när datorn stängs av. Allt som ska sparas måste därför lagras på hårddisk (eller annat lagringsminne).[284]
- ”Data carving” – teknik för att söka och återställa skadade filer, i synnerhet filer som har förlorat den information som beskriver innehållet (metadata), och som därför måste sökas enbart med hjälp av innehållet.[285]
- Extrahera data från krypterade filer.

Sammanfattningsvis påverkas den personliga integriteten eftersom uppgifter som raderats, men som relativt enkelt kan återskapas, fortsatt utgör en integritetsrisk.

283. https://gbhackers.com/computer-forensics-tools/.
284. https://it-ord.idg.se/ord/arbetsminne/.
285. https://it-ord.idg.se/ord/filrekonstruktion/.

6. Hur bra är integritetsskyddet idag?

En viktig fråga givet de utmaningar och risker som beskrivits i föregående avsnitt om teknikutvecklingen är hur bra integritetsskyddet är idag. Har företag, myndigheter och andra organisationer anpassat sitt skydd av personuppgifter så att det går hand i hand med den digitala utvecklingen? I det här kapitlet beskrivs ett antal iakttagelser från olika delar av IMY:s verksamhet. Det handlar om undersökningar vi gjort, om vår och andra dataskyddsmyndigheters tillsynsverksamhet, om anmälda personuppgiftsincidenter, klagomål och begäran om förhandssamråd samt remisser vi svarat på.



6.1 Privata och offentliga verksamheters arbete med dataskydd

Ett år efter att dataskyddsförordningen började tillämpas genomförde IMY en undersökning av hur långt dataskyddsarbetet kommit i svenska företag, myndigheter och andra organisationer. Resultatet visade att de flesta fått grundläggande strukturer och rutiner på plats, men att det fortfarande i många verksamheter saknades ett systematiskt och kontinuerligt arbete. Branscher som hade större utmaningar var generellt kommuner och regioner, transportsektorn, hotell- och restaurangbranschen samt småbolag med mindre än 10 anställda. Genomgående beskrev företag, myndigheter och andra organisationer att de största utmaningarna i dataskyddsarbetet då handlade om att få till fungerande processer i det löpande arbetet och att tolka regelverket.

En undersökning som genomfördes 2019 visade att medborgare har god kunskap om att personuppgifter samlas in och används men upplever sig ha bristande kännedom om hur uppgifterna används. Detta leder till att drygt sju av tio medborgare känner en viss eller stor oro för hur deras personuppgifter används.

IMY:s övergripande bedömning är att det, två och ett halvt år efter att dataskyddsförordningen började tillämpas, fortfarande i många verksamheter finns omfattande brister som rör grundläggande skyldigheter i dataskyddsarbetet. De drygt 500 *sanktionsavgifter* som hittills utfärdats inom EU visar att de vanligaste överträdelserna handlar om att de grundläggande principerna inte följs, att rättslig grund för behandlingen saknas, att enskildas rättigheter inte hanteras som de ska eller att säkerhetsåtgärderna varit otillräckliga.

Drygt 11 000 *personuppgiftsincidenter* har hittills anmälts i Sverige sedan dataskyddsförordningen började tillämpas. En viktig slutsats från anmälningarna är att många incidenter orsakas av den mänskliga faktorn. Det accentuerar behovet av att relevanta it-säkerhetsåtgärder kompletteras med löpande utbildning och andra åtgärder för att öka kunskapen och medvetenheten hos medarbetarna.

Av de drygt 7 500 *klagomål* som skickats in i Sverige rör ungefär en fjärdedel de rättigheter som förordningen ger medborgarna. Den vanligaste rättigheten som berörs i klagomålen är rätten till radering och därefter rätten till information. Andra vanliga klagomål handlar om bristande säkerhet eller att medborgare ifrågasätter om verksamheterna har rätt att hantera personuppgifter på det sätt de gör, det vill säga om det finns rättslig grund.

Bland de *förhandssamråd* som inkommit till myndigheten återfinns flera där verksamheten önskar använda teknik för ansiktsigenkänning och biometriska uppgifter. Totalt sett är det dock få verksamheter som begärt förhandssamråd, vilket tyder på att kompetensen att genomföra konsekvensbedömningar behöver öka.

En av de mest centrala och mest frekvent återkommande synpunkterna i de *remisser* IMY svarat på har rört behovet av att i lagstiftningsarbetet göra en ingående integritetsskyddsanalys. Ju mer genomarbetad nationell lagstiftning som kompletterar dataskyddsförordningen är, desto enklare blir det för företag, myndigheter och andra organisationer att tolka och tillämpa dataskyddsreglerna.

IMY har gjort ett antal undersökningar sedan 2018 i syfte att få en bild av hur det ser ut med integritetsskyddet efter dataskyddsreformens genomförande. Många verksamheter arbetar systematiskt och strukturerat med sitt dataskyddsarbete, men vi kan samtidigt konstatera att det på många håll finns mycket kvar att göra. Att det finns missnöjda medborgare identifieras genom de klagomål som kommer in till myndigheten och brister kan konstateras dels genom de rapporter om personuppgiftsincidenter som löpande anmäls till myndigheten, dels genom de granskningar som myndigheten har genomfört och som har genomförts inom EU från och med den 25 maj 2018 och framåt. I detta kapitel lämnas en sammanfattning av de iakttagelser som hittills gjorts.

6.1.1 Iakttagelser från nationella integritetsrapporten 2019 med mera

Den nationella integritetsrapporten 2019[286] bygger på genomförda undersökningar med medborgare och verksamheter något år efter att dataskyddsreformen genomfördes.[287]

När det gäller verksamheterna var de iakttagelser som gjordes att vissa branscher syntes ha kommit längre i sitt integritets- och dataskyddsarbete än andra. Bland branscher som generellt uppgavs ha kommit längre återfanns exempelvis bank- och finans, it- och telekom, utbildningsföretag och privata vård- och omsorgsföretag. Branscher som hade större utmaningar var generellt kommuner och regioner, transportsektorn, hotell- och restaurangbranschen samt småbolag med mindre än 10 anställda.

Representanter för verksamheterna, oftast dataskyddsombud, bedömde att implementeringen av dataskyddsförordningen gått bra och majoriteten av de tillfrågade uppgav att man hade grundläggande riktlinjer och rutiner på plats. Det som saknades var ett mer systematiskt arbete med integritets- och dataskyddsfrågorna i verksamheten. Det framkom även att den största utmaningen för verksamheterna var att få till fungerande rutiner och processer.

Ytterligare en utmaning för verksamheterna var kopplat till det nya regelverket och tolkningarna av det. Det fanns fortsatt stort behov av stöd och vägledning kring bland annat rättslig grund, säkerhetsåtgärder, regler för kamerabevakning samt gränsdragningen mellan personuppgiftsansvarig och personuppgiftsbiträde. Det konstaterades också att medarbetare behöver fortsatt och kontinuerlig utbildning och kompetensförstärkning i dataskyddsfrågor.

Bilden bekräftas av andra undersökningar och i bland annat rapporten *Sjyst data!* anges att kunskapen och medvetenheten om de nya dataskyddsreglerna har blivit bättre, men fortfarande behöver höjas i de flesta organisationer. Ett problem uppges vara att kunskap om dataskydd inte sällan finns hos en liten grupp av specialister och ibland enbart hos organisationens dataskyddsombud.[288] Detta förstärker bilden av att det fortfarande behövs ett mer systematiskt arbete med integritets- och dataskyddsfrågor i många verksamheter.

Implementeringen av dataskyddsförordningen har av verksamheter i huvudsak bedömts gå bra. Svenskt Näringsliv har dock bedömt att dataskyddsförordningen har medfört stora utmaningar och kostnader för företagen. I många fall har anpassningarna lett till att dataskyddet förbättrats avsevärt. I andra fall har det lett till ökad byråkrati utan någon egentlig förbättring av skyddet för enskilda.[289]

Fortsatt osäkerhet kring vad som är tillåtet kan enligt Svensk Näringsliv ha en tillbakahållande effekt i verksamheterna som går längre än vad som är motiverat för att skydda enskilda. De utmaningar som beskrivs handlar bland annat om vaga och svårtolkade bestämmelser, att det finns brister i harmoniseringen mellan medlemsstaterna som påverkar företag med verksamheter i flera länder negativt, och att det saknas vägledning och råder omfattande oklarheter kring internationella dataflöden.

Utifrån den nationella integritetsrapporten kan sammanfattningsvis konstateras att det 2019 fortfarande fanns mycket kvar att göra i många branscher och att kunskaperna i dataskyddsfrågor behövde förbättras. Medarbetarna uppgavs många gånger utgöra en svag länk och organisatoriska åtgärder i form av utbildning behöver vidtas. Åtgärder behöver också vidtas i syfte att säkerställa att kunskaperna om dataskyddsfrågor breddas i organisationerna. Framför allt är det en ledningsfråga att säkerställa ett systematiskt arbete med integritets- och dataskyddsfrågor i verksamheterna.

286. Datainspektionens rapportserie 2019:2 *Nationell Integritetsrapport 2019*.

287. Här beskrivs hur väl implementeringen genomförts i verksamheterna, medborgarnas upplevelser redovisas i avsnitt 6.2. Verksamheterna omfattade både verksamheter med och utan dataskyddsombud. Slutsatserna var i huvudsak desamma.

288. Vinnova/RISE *Sjyst data!* – Slutrapport november 2019.

289. https://www.svensktnaringsliv.se/bilder_och_dokument/vad-ar-fel-med-gdprpdf_1004995.html/BINARY/Vad%20är%20fel%20med%20GDPR-.pdf.

6.1.2 Iakttagelser utifrån anmälda personuppgiftsincidenter

IMY har sedan 2018 hittills publicerat fyra rapporter som rör anmälda personuppgiftsincidenter.[290] Verksamheter har ett ansvar för att inom 72 timmar efter upptäckt rapportera en personuppgiftsincident till tillsynsmyndigheten.[291]

Antalet anmälda personuppgiftsincidenter som inkommit till IMY uppgår sedan maj 2018 till drygt 11 000. 2018 anmäldes totalt under året knappt 2 300 incidenter, vilket motsvarade cirka 320 incidenter per månad.[292] Under 2019 fick IMY totalt in knappt 4 800 och under 2020 närmare 4 500 anmälningar om personuppgiftsincidenter, vilket motsvarar cirka 375–400 anmälda incidenter per månad.

Det är svårt att dra säkra generella slutsatser om branscher eller områden som är särskilt utsatta för incidenter, då det sannolikt finns ett stort mörkertal. Myndigheten har dock lämnat generella rekommendationer för att verka för en förbättrad personuppgiftshantering i syfte att förebygga incidenter och mildra konsekvenserna om de ändå inträffar.

Generella rekommendationer har varit att rutinerna för att upptäcka och anmäla incidenter kan förbättras ytterligare och att verksamheterna bör använda incidenterna för lärande och utveckling, då incidenterna bör kunna ge viktiga signaler om interna utvecklingsbehov som bör tas tillvara. En förbättrad behörighetsstyrning kan förebygga incidenter genom att risken för obehörig åtkomst och obehörigt röjande minskar.

Rekommendationerna har i övrigt rört behovet av utbildning av medarbetarna. Precis som indikerades i den nationella integritetsrapporten visar även inkomna incidentrapporter att medarbetarna utgör en svag länk. En stor andel incidenter – ungefär hälften av incidenterna – uppges bero på *den mänskliga faktorn*. Detta accentuerar behovet av att styrdokument och tekniska informationssäkerhetsåtgärder kompletteras med löpande utbildning och andra åtgärder för att öka kunskapen och medvetenheten hos medarbetarna. Frågor som särskilt bör adresseras rör e-posthantering, kryptering vid överföring av uppgifter på flyttbara lagringsmedia (som usb-minnen, bärbara datorer och mobiltelefoner) samt att öka kunskapen om antagonistiska angrepp, som ofta sker genom att medarbetare öppnar skadliga länkar eller filer från okända avsändare.

När det särskilt gäller förmågan att stå emot antagonistiska angrepp har IMY pekat på att grundläggande it-säkerhetsåtgärder behöver vidtas i syfte att stärka skyddet för de personuppgifter som hanteras. Exempel på tekniska åtgärder är löpande säkerhetsuppdateringar, uppgradering av mjuk- och hårdvara samt av operativsystem, införande av flerfaktorsautentisering samt användning av antivirusprogram. Även kryptering anges som exempel på lämplig säkerhetsåtgärd i sammanhanget.

Slutsatserna och rekommendationerna ligger väl i linje med de konstateranden som MSB gör mot bakgrund av de allvarliga it-incidenter i offentlig sektor som anmäls till MSB. Statliga myndigheter är sedan 2016 skyldiga att anmäla allvarliga it-incidenter till MSB. I rapporteringen om de knappt 300 allvarliga it-incidenter som anmäldes under 2019 påtalar MSB att antalet rapporterade allvarliga it-incidenter är lågt och att det verkliga antalet sannolikt är högre. MSB:s redovisning visar också att handhavandefel är den vanligaste typen av allvarlig incident och att systematiskt och riskbaserat informationssäkerhetsarbete med incidenthanteringsprocesser och kontinuitetsplanering skulle höja lägstanivån.[293]

290. Datainspektionens rapport 2019:1 *Anmälda personuppgiftsincidenter 2018*, Datainspektionens rapport 2019:3 *Anmälda personuppgiftsincidenter januari – september 2019*, Datainspektionens rapport 2020:2 *Anmälda personuppgiftsincidenter 2019* och Datainspektionens rapport 2020:3 *Personuppgiftsincidenter som beror på antagonistiska angrepp 2019*.

291. En personuppgiftsincident är enligt dataskyddsförordningen artikel 4 punkt 12 en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Hur incidenten ska behandlas regleras i artikel 33–34 i förordningen. Det är allvarligt att underlåta att rapportera inträffade incidenter då verksamheten i sådana fall riskerar sanktionsavgifter vid en ev. granskning av tillsynsmyndigheten (artikel 33–34, samt artikel 83.4 (a) dataskyddsförordningen).

292. Rapporteringsskyldigheten infördes genom att dataskyddsförordningen infördes den 25 maj 2018. Det finns därför inte några siffror för helåret 2018.

293. MSB 1526, *Årsrapport it-incidentrapportering 2019 – Vad har hänt, varför har det hänt, och vad ska göras för att undvika att det händer igen?*

Även rapporten *Cybersäkerhet i Sverige 2020 – hot, metoder, brister och beroenden* påtalar vikten av ett kontinuerligt och systematiskt säkerhetsarbete. I rapporten varnas för att arbetet med cybersäkerhet inte är ändamålsenligt sett till de hot och risker som finns. Exempel på återkommande brister i säkerhetsarbetet är att engagemang, ansvar och ägarskapet för säkerhetsfrågor är lågt, att information inte är korrekt inventerad och klassificerad, att processer, regler och policys saknas eller har brister, att beslutade säkerhetsåtgärder inte genomförs eller att det finns brister i avtal med leverantörer och deras underleverantörer.[294]

Sammanfattningsvis tyder inkomna anmälningar om personuppgiftsincidenter på att det finns behov av att förbättra arbetet med grundläggande informationssäkerhetsåtgärder för att minska riskerna för enskildas fri- och rättigheter i verksamheterna. Att det finns ett generellt behov av att förbättra arbetet med informationssäkerhet är också ett återkommande budskap från andra ansvariga myndigheter.

6.1.3 Iakttagelser utifrån inlämnade klagomål

Myndigheten har sedan 2018 hittills publicerat två rapporter som rör inkomna klagomål.[295] Enskilda individer har enligt dataskyddsförordningen en uttalad rätt att klaga till tillsynsmyndigheten. Antalet klagomål har varit förhållandevis stort i förhållande till antalet klagomål som lämnades till myndigheten åren före dataskyddsreformen genomfördes. Totalt har IMY sedan den 25 maj 2018 tagit emot drygt 7 500 klagomål. De två första åren efter införandet av dataskyddsförordningen tog IMY emot omkring 3 000 klagomål per år. Detta är en väsentlig ökning jämfört med 2017 då myndigheten tog emot knappt 250 klagomål.

Ungefär en fjärdedel av klagomålen avser de rättigheter som förordningen ger medborgarna.[296] Den vanligaste rättigheten som berörs i klagomålen är rätten till radering och därefter rätten till information genom registerutdrag.

Ytterligare en fjärdedel av klagomålen riktas mot personsöktjänster, det vill säga sajter med utgivningsbevis. Sajternas innehav av utgivningsbevis innebär att de har grundlagsskydd och till stora delar är undantagna från reglerna i dataskyddsförordningen. I klagomålen framgår att medborgarna upplever sajternas omfattande publicering av personuppgifter och andra uppgifter om dem och deras levnadsförhållanden som mycket kränkande.

Drygt ett av tio klagomål handlar om att medborgarna upplever att säkerheten i hanteringen av deras personuppgifter brister, till exempel att känsliga personuppgifter mejlas okrypterat. Ytterligare drygt ett av tio klagomål handlar om att medborgare ifrågasätter om verksamheterna har rätt att hantera personuppgifter på det sätt de gör, det vill säga om det finns rättslig grund. Knappt ett av tio klagomål handlar om kamerabevakning och vanligaste klagomålet i det sammanhanget är att medborgare kamerabevakar grannars tomter eller egendom.

6.1.4 Iakttagelser utifrån genomförd tillsyn

IMY har ansvar för att övervaka och granska efterlevnaden av dataskyddsförordningen och genomför även tillsyn vad gäller brottsbekämpande myndigheters personuppgiftshantering, samt inom kreditupplysning och inkasso. När det gäller integritetsaspekterna har ännu förhållandevis få nationella beslut fattats för att kunna dra några sammanfattande och generella slutsatser. Vid en sammanställning av tillsynsbeslut som har fattats inom EU/EES[297] kan dock några generella trender skönjas.

En utgångspunkt vid tillsyn av personuppgiftshanteringen enligt dataskyddsförordningen är att en överträdelse av förordningen som huvudregel ska resultera i en sanktionsavgift. Den kan variera i storlek och kan, om det är frågan om en mindre överträdelse, ersättas med en reprimand. Generellt kan sägas att sanktionsavgifterna kan bli höga.[298]

294. FRA, Försvarsmakten, MSB, Polisen och Säkerhetspolisen; *Cybersäkerhet i Sverige 2020 – hot, metoder, brister och beroenden*.

295. Datainspektionens rapport 2020:1 *Klagomål mot personsöktjänster med frivilligt utgivningsbevis maj 2018–oktober 2019*, Datainspektionens rapport 2020:4 *Klagomål till Datainspektionen 25 maj 2018–24 maj 2020*.

296. Avser perioden 25 maj 2019–24 maj 2020.

297. Dataskyddsförordningen gäller som nämnts för EU:s medlemsstater, samt för EES-länderna Island, Norge och Lichtenstein.

298. För företag kan sanktionsavgiften uppgå till 20 miljoner euro eller 4 procent av den globala årsomsättningen, beroende på vilket som är högst. De höga avgifterna är avsedda att inskärpa betydelsen av att hantera personuppgifter på ett säkert och omsorgsfullt sätt.

6.1.4.1 Tillsyn inom EU

Från och med den 25 maj 2018 till och med den 11 december 2020 har tillsynsmyndigheterna inom EU fattat beslut i 479 ärenden som innehåller sanktionsavgifter.[299] Spanien är det land som utfärdat flest sanktionsavgifter och stod för en tredjedel av meddelade beslut.[300] De 50 lägsta sanktionsavgifterna, som generellt avser enskilda mindre överträdelser, uppgår till mellan 28 och drygt 1 000 euro. De 50 högsta sanktionsavgifterna, som generellt avser överträdelser av flera grundläggande artiklar i förordningen och följer på en mer omfattande granskning, uppgår till mellan 180 000 och 50 miljoner euro.

De fem högsta sanktionsavgifterna uppgår till[301]

- 50 miljoner euro – avser bristande information till enskilda från Google Inc. (FR)
- 35 miljoner euro – avser felaktig hantering av personuppgifter om anställda inom H&M i Tyskland (DE)
- 28 miljoner euro – avser att enskildas rätt till radering och att invända mot personuppgiftsbehandling inte tillgodosetts i ett italienskt telecomföretag (IT)
- 22 miljoner euro – avser omfattande läckage av passageraruppgifter, adress- och bankuppgifter med mera inom flygbolaget British Airways (UK).
- 20 miljoner euro – avser omfattande läckage av personuppgifter inom hotellkedjan Mariott (UK[302]).

Närmare hälften av sanktionsavgifterna, 235 ärenden, är på 10 000 euro eller mer. Av de 479 meddelade besluten omfattar 65 sanktionsavgifter på motsvarande 100 000 euro (drygt 1 miljon svenska kronor) eller mer. Sverige står för åtta av dessa ärenden.

Den största sanktionsavgiften som IMY har beslutat om i Sverige är 75 miljoner kronor och rör bristande borttagande av sökträffar av Google LLC och brister i deras rutiner vid information om borttagande av sökträffar till webbleverantörer. Sanktionsavgiften fastställdes till 52 miljoner kronor av förvaltningsrätten i Stockholm. Domen har överklagats.

Det kan noteras en allt högre aktivitet hos tillsynsmyndigheterna i den meningen att fler beslut fattas och framför allt med höga sanktionsavgifter. Mellan den 1 juli och 11 december 2020 fattades beslut i 156 ärenden med sanktionsavgifter. 28 av de 50 ärendena med högst sanktionsavgifter som har beslutats sedan den 25 maj 2018 har fattats under den perioden. Det tyder på att fler mer omfattande granskningar nu har kunnat avslutas.

Vid en sammanställning av besluten rörande de 50 högsta respektive 50 lägsta sanktionsavgifterna kan utläsas att de överträdelser som har konstaterats till övervägande del i huvudsak handlar om fyra grundläggande faktorer. De avser

- **överträdelser av de grundläggande principerna**, vilket vanligen omfattar överträdelse av själva grundprinciperna, men även att personuppgiftsansvarige inte kunnat visa att de grundläggande principerna följs (ansvarsprincipen)
- **avsaknad av rättslig grund för behandlingen**, antingen att rättslig grund helt saknas eller att den uppgivna rättsliga grunden har tillämpats på ett felaktigt sätt
- att man inte har efterkommit **enskildas rättigheter**, bland annat rätten till information, rättelse och radering samt
- **bristande tekniska och organisatoriska säkerhetsåtgärder** som har medfört att personuppgifter inte har tillförsäkrats den skyddsnivå som är lämplig i förhållande till uppgifternas art, omfattning och det sammanhang de behandlas och risken för enskildas personliga integritet om uppgifterna inte ges tillräckligt skydd.

Det är ingen större skillnad i överträdelsernas karaktär mellan de största och minsta sanktionsavgifterna men bristande säkerhet var mindre vanligt förekommande vid de mindre överträdelserna. Detta kan tyda på att de mindre överträdelserna baserar sig på enskilda klagomål där framför allt enskildas rättigheter aktualiseras. Ett antal överträdelser rör också konsekvensbedömning och förhandssamråd, respektive brister i incidentanmälningar.

299. https://www.enforcementtracker.com/. Sammanställningen är gjord utifrån de uppgifter som är inhämtade i tjänsten Enforcement Tracker per den 11 december 2020 (vid årsskiftet hade antalet sanktionsbeslut passerat 500). Enskilda beslut är inte inhämtade, återgivningen är därför indikativ och används för att illustrera utvecklingen. I tjänsten anges inledningsvis belopp som tillsynsmyndigheten beslutat om. Detta justeras om nationell domstol fastställt ett annat belopp. Det framgår dock inte om så har skett och i vilken instans ändring har skett eller om sanktionsbeloppet har vunnit laga kraft.

300. Spanien stod ensamt för 169 av de 479 besluten. Spanien har haft möjlighet att besluta om sanktionsavgifter enligt sin nationella lagstiftning redan före dataskyddsförordningen, vilket sannolikt är en förklaring till detta.

301. Mot bakgrund av att regelverket är nytt och att merparten av tillsynsmyndigheterna har fått möjlighet att besluta om sanktionsavgifter och andra mer ingripande korrigerande befogenheter först genom dataskyddsförordningen, saknas ännu i stor omfattning lagakraftvunna beslut från högre instans i nationella domstolar.

302. Den brittiska dataskyddsmyndigheten har meddelat fyra beslut med sanktionsavgifter, varav två ingår i de fem högsta avgifterna. De andra besluten var också förhållandevis stora och omfattade sanktionsavgift om 1,4 miljoner euro (Ticketmaster UK) respektive 320 000 euro (Apotek).

6.1.4.2 Tillsynsbeslut från IMY

Sedan den 25 maj 2018 har IMY fram till och med årsskiftet 2020 avslutat omkring 150 tillsynsärenden.

Under 2019 avslutades två ärenden med sanktionsavgifter. Under 2020 har 15 ärenden avslutats med sanktionsavgifter. Ungefär hälften av dessa ärenden är överklagade, varför sanktionsavgifterna kan komma att ändras. Beloppen nedan anger IMY:s ursprungliga beslut.

En kort beskrivning av de svenska beslut som lett till sanktionsavgifter ges i det följande.[303]

Några beslut har rört kamerabevakning. Ett ärende avsåg användning på försök av ansiktsigenkänningsteknik för närvarokontroll på en skola. Bristerna avsåg den grundläggande principen om uppgiftsminimering, behandling av känsliga personuppgifter samt avsaknad av konsekvensbedömning och förhandssamråd (sanktionsavgift 200 tkr)

Två beslut rör kamerabevakning i fastigheter eller i enskildas boenden. En bostadsrättsförening använde kamerabevakning i entré och trapphus med mera i syfte att komma tillrätta med bland annat ordningsstörningar och skadegörelse. Bristerna rörde de grundläggande principerna, avsaknad av rättslig grund samt bristande information (sanktionsavgift 20 tkr). Även i en hyresfastighet användes kamerabevakning i trapphuset i syfte att komma tillrätta med skadegörelse. Bristerna handlade här om bristande rättslig grund (sanktionsavgift 300 tkr). Slutligen finns ett ärende som rör övervakning av en boende på ett LSS-hem i dennes sovrum. Bristerna avsåg de grundläggande principerna, avsaknad av rättslig grund, behandling av känsliga personuppgifter, bristande information och skyltning, samt avsaknad av konsekvensbedömning och förhandssamråd (sanktionsavgift 200 tkr).

Besluten pekar på att integritetsintresset generellt väger mycket tungt i enskildas boendemiljö och att det krävs omfattande analyser och att alternativa, mindre ingripande, åtgärder än kamerabevakning undersöks och används som huvudregel. Användning av ansiktsigenkänning, som innehåller biometriska uppgifter, innebär som tidigare beskrivits generellt höga risker för den personliga integriteten. En konsekvensbedömning och förhandssamråd med tillsynsmyndigheten ska i sådana fall genomföras innan man påbörjar behandlingen. Det har också konstaterats att det saknas undantag för testverksamhet med skarpa personuppgifter i dataskyddsregleringen.

Ett ärende rör behandling av uppgifter om lagöverträdelser. En masspubliceringssajt tillhandahöll kreditupplysningsinformation och samtidigt uppgifter om lagöverträdelser. Uppgifter om lagöverträdelser får inte behandlas i kreditupplysningsverksamhet. Bolaget saknade därmed rättslig grund för behandling av uppgift om lagöverträdelser i kreditupplysningsverksamheten och överträdde även grundläggande principer (sanktionsavgift 35 000 euro).

Google-ärendet rörde enskildas rättigheter. Google LLC hade inte tagit bort två sökträffar som IMY tidigare förelagt Google att ta bort samt publicerade webbmeddelanden till de hemsidor där borttagning av sökträffar skedde. Bristerna var hänförliga till de grundläggande principerna, avsaknad av rättslig grund och enskildas rätt att bli raderad, rätten att bli bortglömd (sanktionsavgift 75 mkr).

Flera ärenden bottnade i en personuppgiftsincidentanmälan (eller avsaknad av sådan). Ett sådant fall var en myndighet som inte agerat på en personuppgiftsincident i tid och på ett tillräckligt genomgripande sätt (sanktionsavgift 185 000 kr). Generellt leder en utebliven eller sen anmälan om personuppgiftsincidenter till sanktionsavgift. Besluten har också tydligt pekat på vikten av att dokumentera incidenten och bedömningarna som gjorts i samband med den, då verksamheten har krav på sig att visa att hanteringen varit korrekt.

Flera beslut har rört bristande säkerhet i form av tekniska och organisatoriska åtgärder. Ett fall rörde en kommun som i samband med publicering av protokoll publicerade känsliga personuppgifter om en enskild individ på kommunens webbplats. Bristerna rörde de grundläggande principerna, behandling av känsliga personuppgifter och avsaknad av rättslig grund (sanktionsavgift 120 tkr). Ett annat fall rörde forskare som skickat känsliga forskningsuppgifter över okrypterad mail och lagrat ett antal förundersökningsprotokoll med känsliga uppgifter, som ingick i forskningen, i en molntjänst. Bristerna var hänförliga till de grundläggande principerna, bristande säkerhet och bristande personuppgiftshantering (sanktionsavgift 4 mkr). Ytterligare ett fall rörde incidenter i fem olika delsystem i en skolplattform. Brister hade funnits över längre tid och även känsliga och integritetskänsliga uppgifter, exempelvis uppgifter om skyddad identitet, hade förekommit. Bristerna avsåg de grundläggande principerna, bristande säkerhet i plattformen samt bristande konsekvensbedömning (sanktionsavgift 4 mkr).

303. Här är det centralt att notera att sanktionsavgifternas storlek varierar beroende på om det är frågan om en myndighet eller privat verksamhet. För myndigheter är avgiftens storlek max 10 miljoner kronor, för privata verksamheter max 20 miljoner euro eller max 4 procent av den globala årsomsättningen, beroende på vilket som är högst. Faktorer som ska beaktas vid fastställandet av sanktionsavgiftens storlek anges i artikel 83 dataskyddsförordningen.

Det ställs stora krav på att verksamheter anpassar skyddet för de personuppgifter som behandlas utifrån uppgifternas omfattning, karaktär och art och att de löpande vidtar relevanta tekniska och organisatoriska åtgärder för att säkerställa skyddet för uppgifterna. Besluten visar också på behovet av att säkerställa att medarbetare vet hur uppgifter får behandlas och följer verksamhetens instruktioner.

Sju ärenden riktades mot fyra offentliga och tre privata vårdgivare som inte uppfyllt kraven på att göra en behovs- och riskanalys innan tilldelning av behörigheter i deras respektive patientjournalsystem. Bristerna rörde de grundläggande principerna och bristande säkerhet genom avsaknad av den organisatoriska åtgärden att utföra en behovs- och riskanalys innan tilldelning av behörigheter. Totalt omfattade granskningen åtta vårdgivare. Ett ärende avslutades med ett föreläggande. Sanktionsavgifterna uppgick för de privata vårdgivarna till mellan 15 och 30 miljoner kronor och för de offentliga vårdgivarna till mellan 2,5 och 4 miljoner kr.

Sammanfattningsvis kan konstateras att de övergripande brister som framkommit i de svenska tillsynsärenden som lett till sanktionsavgift speglar de generella brister som tidigare uppmärksammats genom anmälda personuppgiftsincidenter och inkomna klagomål. Bristerna rör de grundläggande principerna, att man saknar rättslig grund för behandlingen, att man inte genomfört konsekvensanalys inför omfattande eller nya behandlingar, att personuppgiftsincidenter inte anmälts eller dokumenterats, att man inte har efterkommit enskildas rättigheter, samt att det finns bristande tekniska och organisatoriska säkerhetsåtgärder som har medfört att personuppgifter inte har tillförsäkrats ett tillräckligt skydd.

6.1.5 Iakttagelser utifrån meddelade förhandssamråd

Ett förhandssamråd behöver genomföras om en verksamhet har gjort en konsekvensbedömning och därefter har vidtagit integritets- och säkerhetshöjande åtgärder och fortfarande bedömer att risken för enskildas integritet är hög.[304] IMY har sedan den 25 maj 2018 respektive 1 augusti 2018 fått in begäran om förhandssamråd som lett till yttrande i sak i ett drygt 10-tal ärenden.

Flera ärenden har rört användning av kamera och kamerateknik. Ett ärende rörde avläsning av registreringsskyltar på fordon med fasta kameror för automatisk kameraavläsning av registreringsnummer på fordon på avgränsade platser för jämförelse med uppgifter i myndighetens befintliga underrättelseregister för brottsbekämpning. Vid en ”träff” skulle uppgifter kommuniceras i realtid till berörda tjänstemän. Inga uppgifter skulle lagras. Ett annat ärende rörde förhandssamråd inför användningen av ny programvara för ansiktsigenkänning som skulle samköras mot annat register. De biometriska uppgifterna skulle enbart behandlas inom en specifik del av verksamheten. Ytterligare ett ärende rörde planerad användning av bildanalysverktyg vid utredning av brott. Förhandssamråd har också begärts inför en planerad pilotverksamhet med biometrisk ansiktsverifiering vid yttre gräns som innebar insamling av ansiktsbilder från flygpassagerare på flygplatsen och jämförelse av dessa bilder mot passagerares resehandling i syfte att kontrollera resehandlingens äkthet och personens identitet.

IMY har generellt bedömt att det funnits berättigat intresse av att behandla uppgifterna, men har lämnat ett antal råd. De har bland annat rört behovet att beakta den grundläggande principen om uppgiftsminimering, behovet av att säkerställa tillräckliga tekniska och organisatoriska åtgärder och att överväga om syftet med behandlingen i vissa fall skulle kunna uppnås på ett annat sätt, med mindre integritetsintrång, än med stöd av den tänkta metoden. Råden har också avsett att vidta ytterligare åtgärder för att begränsa intrånget i den enskildes personliga integritet. Myndigheten har också lämnat it-säkerhetsmässiga råd om exempelvis åtkomstskydd, loggning och logguppföljning samt rutiner för behörighetstilldelning. Råden har också omfattat lagring och gallring samt rutiner för registervård. Myndigheten har slutligen också lämnat råd rörande nödvändigheten i att tillgodose de registrerades rättigheter – rätt till information och rätt till rättelse med mera. Betydelsen av att tydligt informera besökarna om behandlingen och deras möjligheter att invända mot behandlingen framhölls särskilt i ett ärende rörande besökares rörelsemönster i butik.

304. Det är större krav på att genomföra förhandssamråd i brottsbekämpande verksamhet, genom att det i stället för ”hög” kvarvarande risk, enbart krävs ”särskild risk” för intrång i den personliga integriteten för att ett förhandssamråd ska behöva genomföras, 3 kap. 7 § brottsdatalagen.

I ett par fall har råden rört behovet av att tydliggöra ansvarsfördelningen mellan olika aktörer i samband med behandlingen.

Förhandssamråd har också omfattat användande av ett verktyg för att följa beteendemönster på en dator och särskilt en funktion för ansiktsigenkänning i samband med examination på distans i syfte att säkerställa studenters identitet. Då det bedömdes saknas lagstöd för en sådan behandling lämnade IMY råd om att undersöka mindre integritetskänsliga metoder för att identifiera studenterna och att säkerställa att den lösning som väljs inte innebär ett betydande intrång i den personliga integriteten.

I samband med inspelning av telefonintervjuer i kvalitets- och uppföljningssyfte har myndigheten lämnat råd som handlar om att säkerställa att det finns rättslig grund för behandlingen och att principen om uppgiftsminimering beaktas genom att inte samla in fler uppgifter än vad som är nödvändigt för att uppnå syftet. Även i detta sammanhang har råd lämnats om tydlig information, radering, samt åtkomstkontroll och behörighetsstyrning.

Sammanfattningsvis kan konstateras att det hittills har varit frågan om förhållandevis få förhandssamråd som hanterats av IMY sedan dataskyddsregleringen infördes 2018. Givet den snabba tekniska utvecklingen och att kraven på konsekvensbedömning[305] borde träffa ett stort antal verksamheter, behandlingssituationer och utvecklingsinitiativ som idag pågår, kan konstateras att det sannolikt finns ett stort mörkertal kring såväl konsekvensbedömningar som förhandssamråd. Några av de tillsynsärenden som har avslutats visar också på brister när det gäller konsekvensbedömning och förhandssamråd.

6.2 Oron för hur personuppgifter används ökar

I den nationella integritetsrapporten 2019 riktades en större undersökning till medborgare. IMY kunde konstatera att dataskyddsförordningen var relativt välkänd bland medborgarna, att det fanns en god kunskap om att personuppgifter samlas in och används, men att det fanns en lägre kännedom om hur uppgifterna används. Detta leder till att drygt sju av tio medborgare känner en viss eller stor oro för hur deras personuppgifter används.

Enligt undersökningen anser medborgare att finansiella uppgifter och hälsoppgifter är särskilt känsliga och det finns en uttalad och återkommande oro kring att använda sitt bankkort på nätet. Även insamling av personuppgifter för riktad reklam skapar oro. Förtroendet för olika verksamheters hantering av personuppgifter varierar i stor utsträckning. Störst förtroende har medborgarna för personuppgiftshanteringen inom vård, myndigheter och banker. Lägst förtroende åtnjuter appar, sociala medier och sökmotorer.

Det finns demografiska skillnader i vilken kunskap som finns, hur stor oro man har och hur man skyddar sina personuppgifter. Vuxna personer i åldern upp till 39 år och högskole- och universitetsutbildade känner i högre grad till dataskyddsförordningen, vad de har för rättigheter och hur deras personuppgifter används. Äldre, och personer med låg utbildning upplever sig i större omfattning ha lägre kunskap om hur deras personuppgifter används, och upplever även större oro. Den del av befolkningen som använder internet sällan eller inte alls utgörs i högre grad av äldre, personer med lägre hushållsinkomst och utbildning, kvinnor samt boende på landsbygden.

I rapporten *Sjyst Data!* anges också att ökad kunskap om hur datadelning går till ökar villigheten att dela vissa data. Det framkommer också att 59 procent av svenskarna är negativa till företags insamling, men att de med högre kunskap i högre utsträckning gör aktiva val för att till exempel kunna surfa anonymt och samtidigt är mer positiva till registrering. IMY:s undersökning tyder också på att ökad kunskap medför att man i ökad utsträckning anammar de nya rättigheter som dataskyddsförordningen medfört. Bland personer i åldern 18–29 år har 22 procent utnyttjat någon av rättigheterna i dataskyddsförordningen jämfört med 16 procent i befolkningen som helhet.

305. Se närmare om konsekvensbedömning, bilaga 1.

En slutsats i rapporten *Sjyst data!* är att en ökad trygghet – som kommer av vana, frekvent användning och kunskap – tycks påverka hur positiv man är till att dela med sig av sina data vilket sannolikt innebär att internetanvändares inställning kan påverkas över tid genom ökad kunskap och ökad användarvana.

I den senaste upplagan av *Svenskarna och internet* framkommer att pandemin har haft effekt på medborgarnas oro. Allt fler har jämfört med tidigare mätningar uppgivit att de känner sig oroade över att få sin integritet kränkt av storföretag på nätet, men också av myndigheter. Känslan av att vara övervakad på nätet har vuxit under pandemin. I rapporten konstateras också att oron är betydligt högre för den digitala integriteten bland dem i privat sektor jämfört med dem offentlig sektor. Generellt är enligt rapporten män mer oroliga än kvinnor över att få sin digitala integritet kränkt på nätet.[306]

Trots oron och en medvetenhet om att man behöver värna sina personuppgifter delar många med sig av sina personuppgifter. Detta brukar kallas för integritetsparadoxen. Anledningen till att man delar med sig av uppgifterna trots upplevd oro varierar, men många gånger bedöms tillgången till den tjänst som erbjuds vara så attraktiv att oron får stå tillbaka. Det saknas i vissa fall också kunskap om hur man kan skydda sina uppgifter. Alternativet blir då att antingen dela sina uppgifter eller helt avstå från tjänsten. Den nationella integritetsundersökningen visar att män och personer i åldern 18-29 år är överrepresenterade bland dem som ibland eller alltid gör aktiva val för att undvika att surfvanor samlas in medan kvinnor och personer i åldern 65-79 är överrepresenterade bland dem som uppger att de ofta eller ibland helt avstår från att använda en digital tjänst om de känner osäkerhet kring hur deras personuppgifter kommer att hanteras.

306. Internetstiftelsen; *Svenskarna och Internet 2020*, internetstiftelsen-svenskarna-och-internet-2020.pdf.

6.3 Integritetsskyddet i lagstiftningsprocessen – vanliga remissynpunkter

IMY har de senaste åren årligen svarat på ett stort antal remisser och delningar. Aktiviteten var särskilt stor i samband med anpassningen av nationell rätt till dataskyddsreformen, då all nationell reglering som rör behandling av personuppgifter behövde anpassas till förordningen och dataskyddslagen och implementeringen av brottsdatadirektivet. Myndigheten deltar även med experter i centrala statliga utredningar där myndighetens sakkunskap är särskilt efterfrågad. Därutöver konsulteras myndigheten ofta under hand i statliga utredningar.

Lagstiftaren har en central roll i att beakta integritetsskyddsaspekter i lagstiftningsarbetet. Detta är särskilt centralt då det många gånger finns en stor komplexitet i regelverken. Det kan vara ett komplext samspel mellan

- **dataskyddsförordningen** – som är primärt regelverk när det gäller personuppgiftsbehandling,
- **dataskyddslagen** – som kompletterar dataskyddsförordningen och innehåller närmare nationella föreskrifter, men är subsidiär i förhållande till annan nationell reglering,
- **brottsdatalagen och särskilda registerförfattningar på det brottsbekämpande området** – som gäller för brottsbekämpande verksamhet,
- **sektorspecifika unionsrättsakter** – som ofta har ett begränsat sektorsperspektiv och många gånger förhandlas inom det departement som ansvarar för respektive sakfråga och som genomförs genom nationella bestämmelser,
- **sektorsspecifika regelverk** – som kompletterar dataskyddsförordningen och tas fram inom ansvarigt departement där sakfrågan står i fokus,
- **eventuella kollektivavtal** – som reglerar förhållandena mellan arbetsmarknadens parter och som också kompletterar dataskyddsförordningen i de delar som rör dataskydd samt
- **offentlighets- och sekretesslagen** – som ibland medför hinder mot att uppgifter lämnas ut till annan part om sekretessbrytande bestämmelser saknas (även om ändamålen i och för sig skulle medge att utlämnande sker).

En av de mest centrala och mest frekvent återkommande remissynpunkterna från IMY har rört behovet av att i lagstiftningsarbetet göra en integritetsskyddsanalys. Myndigheten har återkommande också angett att lagstiftaren med fördel kan göra en konsekvensanalys avseende dataskydd i syfte att identifiera risker och, vid behov, införa lämpliga skyddsåtgärder i lagstiftningen i syfte att minska riskerna och säkerställa de enskilda individers grundläggande rättigheter.

6.3.1.1 En integritetsskyddsanalys bör genomföras vid lagstiftning

En väl genomarbetad lagstiftningsprodukt som har tagit ställning till integritetsskyddsaspekterna förenklar i många fall för företag myndigheter och andra organisationer som i nästa steg ska tillämpa lagstiftningen och minskar risken för tolkningsproblem.[307]

Vanligen genomförs någon form av analys inom ramen för utredningsarbetet. Behoven är ofta väl beskrivna, medan integritetsriskerna kan vara mindre ingående berörda. Ofta saknas själva analysen av hur integritetsintrånget, efter att relevanta säkerhets- och skyddsåtgärder har föreslagits som begränsar intrånget, bedöms stå i proportion till behoven. En analys är en förutsättning för att en relevant proportionalitetsbedömning ska kunna genomföras. Analysen behöver därför vanligen fördjupas i lagstiftningsärenden där frågor om personuppgiftsbehandling aktualiseras. Saknas analysen i lagstiftningsarbetet riskerar regelverket ytterst att inte uppfylla kraven enligt regeringsformen och EU-rätten.

Vid genomförandet av en integritetsskyddsanalys behöver en kartläggning göras av bland annat vilken personuppgiftsbehandling som ska genomföras, av vem och vilka aktörer som kommer att vara personuppgiftsansvariga. Det är också centralt att fastställa och tydliggöra ändamålen med behandlingen, eftersom ändamålen utgör ramen för vilken behandling som kan anses nödvändig.

En integritetsskyddsanalys syftar till att svara på frågan om intrånget i den personliga integriteten är proportionerligt i förhållande till det man avser att uppnå med den föreslagna personuppgiftsbehandlingen. I det ingår att bedöma om behandlingen av personuppgifter är:

- nödvändig utifrån de avsedda ändamålen med behandlingen,
- om det finns alternativa vägar att nå samma resultat men som är mindre integritetskänsliga och
- om det finns integritetshöjande bestämmelser (skyddsåtgärder) som kan behövas för att de grundläggande principerna i dataskyddsförordningen ska uppfyllas och åtgärder för att uppfylla bestämmelserna om inbyggt dataskydd och dataskydd som standard.

Exempel på lämpliga skyddsåtgärder kan vara bestämmelser för att begränsa insamlingen och spridningen av uppgifterna, preciserade gallringsregler samt krav på säkerhetsåtgärder såsom kryptering vid överföring via öppet nät och stark autentisering för åtkomst till känsliga personuppgifter och uppgifter om lagöverträdelser. Även sekretess till skydd för den enskilde används ofta som integritetshöjande åtgärd.

6.3.1.2 Även en konsekvensbedömning kan lämpligen genomföras i lagstiftningsarbetet

I dataskyddsförordningen finns bestämmelser om att den personuppgiftsansvarige ska göra en konsekvensbedömning innan särskilt riskfyllda behandlingar påbörjas.[308] Integritetskommittén föreslog att man även borde införa ett krav i kommittéförordningen på redogörelse av integritetskonsekvenser om förslagen i ett betänkande innebär ett betydande intrång i den personliga integriteten.[309] Något sådant krav har ännu inte genomförts.

307. Ett intrång i enskildas privata sfär som innefattar behandling av personuppgifter måste uppfylla kraven i regeringsformen, Europakonventionen och EU:s rättighetsstadga samt bestämmelserna i EU:s dataskyddsreglering. För att uppfylla kraven i ett konkret lagstiftningsärende krävs att det intrång som sker i den enskildes privata sfär är nödvändigt, befogat och inte större än nödvändigt. Intrånget ska mötas av integritetshöjande bestämmelser till förmån för den enskilde. En följd av denna reglering är bland annat att lagstiftaren har att tydligt redovisa vilka avvägningar som gjorts vid proportionalitetsbedömningen.

308. Se bilaga 1 till rapporten för en närmare beskrivning av kraven på konsekvensbedömning.

309. Regleringen i 2 kap. 6 § andra stycket regeringsformen ger skydd mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

En konsekvensbedömning i ett lagstiftningsärende gör kommande tillämpning mer förutsägbar. Detta är särskilt välkommet när det gäller behandlingar som är nödvändiga för att fullgöra en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.[310] Har en konsekvensbedömning gjorts i lagstiftningsärendet behöver en förnyad konsekvensbedömning inte heller göras av de verksamheter som ska behandla personuppgifter.[311]

Sammanfattningsvis kan konstateras att integritetsanalyser och konsekvensbedömningar avseende dataskydd har betydelse för att säkerställa en väl avvägd lagstiftning som uppfyller kraven i regeringsformen, europakonventionen och EU-rätten, men också för att underlätta tillämpningen. I den mån lagstiftning som rör behandling av personuppgifter inte tillräckligt tydligt uttalar för vilket ändamål uppgifter får behandlas riskerar verksamheterna att sakna lagstöd för sina personuppgiftsbehandlingar.

Alltmer djuplodande integritetsanalyser syns allt oftare i lagstiftningsprodukterna vilket är positivt. Men här finns mer att göra och sannolikt behövs stöd till kommittéväsendet och övriga lagstiftningskedjan för att stärka lagstiftningsprocessen både när det gäller integritetsanalyser och konsekvensbedömningar, men också för att komplettera dataskyddsförordningen i den utsträckning det behövs för att verksamheter ska kunna bedriva sin verksamhet på ett ändamålsenligt sätt och i enlighet med dataskyddsreglerna. Bland annat kan ställas krav på en integritetsanalys redan vid utformningen av kommittédirektiv.

310. Se artikel 6.1 (c) resp. (e) dataskyddsförordningen. Av relevans i lagstiftningssammanhang är även artikel 6.2, 6.3 och skäl 41 i dataskyddsförordningen samt artikel 35.10 dataskyddsförordningen.

311. Artikel 35.10 dataskyddsförordningen.

6.4 Sammanfattning och slutsatser om hur bra integritetsskyddet är idag

Utifrån de underlag som har redovisats ovan kan sammanfattningsvis konstateras att medborgarnas oro för hur deras personuppgifter hanteras ökar. Genomförda tillsyner, inkomna klagomål och rapporter om personuppgiftsincidenter bekräftar att oron kan vara befogad. IMY:s bedömning är sammanfattningsvis att det fortfarande finns omfattande brister som rör grundläggande faktorer när det gäller data- och integritetsskydd. Granskade verksamheter har generellt haft utmaningar i att uppfylla de grundläggande principerna och har ibland saknat rättslig grund för sina behandlingar. De har inte haft tillräcklig säkerhet för sina uppgifter och har i vissa fall inte heller implementerat rutiner och processer och utbildat medarbetarna för att de ska kunna bidra till att upprätthålla skyddet för uppgiftssamlingarna. En förklaring kan vara att det är en konsekvens av att kunskapen om integritets- och dataskyddsfrågorna är begränsad till få och att verksamheterna inte arbetar med dataskyddsfrågor på det systematiska sätt som är en förutsättning för att kunna säkerställa ett adekvat skydd för uppgifterna.

En förklaring kan också vara att de ökade kraven på verksamheterna har införts stegvis och att efterlevnaden av dataskyddsreglerna tidigare till delar har brustit. Det innebär att den digitala utvecklingen när dataskyddsförordningen började tillämpas redan hade kommit långt och att affärsmodeller, avtal och processer inte med enkelhet har kunnat ställas om för att uppfylla samtliga krav enligt förordningen. Integritetsfrågorna riskerar då att bli en fråga om att försöka lägga på ett raster med integritetsskydd, lappa där det går och släcka bränder när de uppstår.

Detta understryker vikten av att verksamheterna arbetar systematiskt med frågorna, att verksamheten anpassas i grunden och att integritetsperspektivet finns med och byggs in i verksamhetssystem och affärsmodeller från början. Särskilt viktigt är detta perspektiv i unga branscher där innovationer testas och en snabb utveckling sker. Saknas integritetsperspektivet från början är det en svår och kostsam process att läka brister i efterhand. Ytterst utsätts medborgarna för risker för sina grundläggande fri- och rättigheter.

Även kommittéväsendet och lagstiftaren har en viktig roll i att säkerställa att lagstiftningsprodukterna håller hög kvalitet där integritetsskyddsanalysen är ett viktigt instrument för att säkerställa att lagstiftningen är proportionerlig. Genomförs konsekvensanalyser i samband med lagstiftningsåtgärder kan integritetshöjande åtgärder genomföras redan i lagstiftningssammanhanget, vilket många gånger bidrar till en korrekt och rättssäker tillämpning.

7. Aktuell forskning om ny teknik och integritetsskydd

I det här avslutande kapitlet beskriver vi några olika svenska undersökningar och forskningsinitiativ som tar sikte på utvecklingen av ny teknik och integritetsskydd.



7.1 Några olika svenska undersökningar och forskningsinitiativ

Färsk svensk forskning har identifierat flera riskområden när det gäller personlig integritet, bland annat när det gäller AI. Men i den akademiska världen finns också ett antal pågående projekt och initiativ som på olika sätt syftar till att höja integritetsskyddet.

Ett område som flera lärosäten forskar om är *transparens* och nya verktyg för att öka användarnas kunskap om och kontroll över vilka personuppgifter som samlas in och används – av vem, på vilket sätt samt eventuella konsekvenser av användningen.

***Integritet vid användning av appar* har stått i fokus i flera studier och rapporter.**

När det gäller *inbyggt dataskydd och dataskydd som standard* har forskare arbetat fram onlineutbildningar i dataskydd, bland annat en med särskild inriktning mot inbyggt dataskydd.

Forskning pågår också för att utveckla *säkra molntjänster och appar*. Målet är att i en molnlösning kunna erbjuda säker analys av känsliga data som till exempel patientuppgifter.

Flera pågående forskningsprojekt syftar till att höja säkerheten i *Internet of things, IoT*. Det handlar bland annat om att höja integritetsskyddet för *IoT* i hemmet och ge individer större kontroll över de uppkopplade enheterna.

Det akademiska intresset för *AI* är stort. En kartläggning från 2019 uppskattade antalet forskningsmiljöer i Sverige som fokuserar på AI till närmare 40. Identifierade problemområden med AI som forskningen menar behöver hanteras ur ett integritetsperspektiv handlar om risken för partisk AI och missbruk men också att säkerställa ansvarsfrågor och transparens.

Det pågår idag ett antal undersökningar och forskningsinitiativ inom digitalisering och ny teknik samt inom integritets- och dataskyddsområdet. Forskning är efterfrågad och bidrar till lärande och kunskapshöjning, ger förslag på nya lösningar och pekar ibland också på områden som behöver fördjupad genomlysning.

Vid en genomgång framkommer att det i forskningen identifieras flera riskområden när det gäller integritetsskydd. En del av forskningen syftar till att möta dessa, bland annat genom att undersöka hur medborgarnas rättigheter kan tillgodoses, lämna förslag på hur verksamheterna kan ta sitt ansvar för integritetsskyddet, eller på annat sätt bidra till att lösa en del av de integritetsrisker som uppmärksammats. Några sådana forskningsinitiativ lyfts fram i det följande.[312]

Avsnittet syftar till att ge exempel på olika sätt som forskning och utveckling bidrar till ett tryggt informationssamhälle. Det förtjänar dock att understrykas att IMY inte gjort någon bedömning av de olika undersökningar och studier som beskrivs.

7.1.1 Skapa förtroende och tillit - genom bland annat verktyg för transparens och certifiering

Ett område som flera lärosäten forskar om är transparens. Flera initiativ tillhandahåller verktyg för transparens i syfte att öka användarnas kunskap om och kontroll över vilka personuppgifter som samlas in och används – av vem, på vilket sätt samt eventuella konsekvenser av användningen.

Ett forskningsinitiativ föreslår en ”katalog” av designriktlinjer som kan ligga till grund för hur information kan utformas för att möta individuella användares behov. Förslag lämnas också på utformning av ett integritetsmeddelande som kan användas för att informera användare om incidenter.[313] Ett annat syftar till att ge kunskap och kontroll om insamlad data och dess användning genom till exempel modeller som beräknar hur integritetsvänliga appar är, eller genom appar som redovisar vilka personuppgifter företag som stora sociala medieaktörer, till exempel Facebook, använder sig av. Forskare i den här gruppen har tagit fram två appar som kan hjälpa privatpersoner att se vilken personlig data företag använder sig av och verkar för att utveckla verktygen ytterligare.[314]

312. Sammanställningen gör inte anspråk på att vara heltäckande, utan ger endast en bild av forskningsresultat som har kommit från olika lärosäten. Karlstad, Lund och Malmö universitet synes vara några av de som har kommit längst i sin forskning inom områden som berör integritets- och dataskydd.

313. P. Murmann, *Towards Usable Transparency via Individualisation*, Karlstads universitet, 2019

314. Projektet drivs inom ramen för Privacy Flag och avser, med avstamp i dataskyddsförordningen, stärka skyddet för fysiska personer vid behandling av personuppgifter inom EU. A. Stålbröst, A. Padyab, *Ta reda på hur företag använder data du delar*. Luleå tekniska universitet, 2018.

Digitaliseringen av handeln gör den mer effektiv och ökar tillväxten. Samtidigt känner konsumenter en oro över bristande transparens, vilket kan skada den tillit mellan handlare och kund som är central i en fungerande marknad. En studie har visat att många konsumenter upplever en bristande kontroll över sina data och att svenska handlare kan göra mer för att stärka kundernas förtroende. Projektet syftar till att bättre förstå relationen mellan tillit och transparens när det gäller kommersiell insamling av konsumenters data.[315]

Den tidigare nämnda rapporten *Sjyst data!* syftar till att lösa en del av konflikten mellan ökad dataanvändning och bevarad personlig integritet och till att skapa ökat förtroende och tillit hos användarna genom en integritetscertifiering vid datainsamling. En sjyst data-certifiering visar att man följer gällande lagar och regler, men också att man tar hänsyn till etiska principer och värnar användarens personliga integritet. Certifieringen skulle kunna användas i stället för, eller parallellt med, andra mekanismer enligt dataskyddsförordningen som syftar till att visa att förordningen följs.[316]

7.1.2 Integritet vid användning av mobilappar

Ett forskningsprojekt visar att information om en persons mobilappar skapar ett unikt digitalt fingeravtryck. I en population på 3,5 miljoner användare var 99,7 procent unika i vilka appar de använde. Möjligheten att få fram sådana digitala fingeravtryck väcker därför frågan om hur en persons integritet ska skyddas.

Forskningen visade att det endast krävdes fyra appar från en mobilanvändare, valda efter popularitetsrankning, för att kunna identifiera över 90 procent av användarna via ett digitalt fingeravtryck. För 10 procent krävdes fler appar för att det digitala fingeravtrycket skulle skapas. Via det digitala fingeravtrycket kunde man avgöra en persons ålder, kön, religion och sexuella läggning. Det som tidigare betraktades som statistik utgör därför enligt forskarna idag mycket känslig information, eftersom en individs identitet kan avslöjas och utnyttjas, till exempel i ovälkomna reklamsammanhang eller påverkanskampanjer. Det kan också vara frågan om mer allvarliga missbruk. Som exempel anges Trumps kampanjorganisations köp av Cambridge Analyticas tjänster i samband med valet 2016. Företaget använde Facebookdata för att profilera och rikta meddelanden till 87 miljoner personer människor. De använde en psykologisk modell för profilering. Enligt forskningen kan digitala app-fingeravtryck profilera på samma sätt. Forskningen pekar också ut risker med tekniken i samband med till exempel utpressning och identitetsstöld. För att användningen av appar och de möjligheter de ger ska kunna vara till stor hjälp i samhället behövs enligt forskarna etiska riktlinjer för designers och app-utvecklare som tar hänsyn till både teknik, integritet och etik.[317]

Appar har blivit en viktig del i våra liv. För att fungera registrerar de många gånger var vi är, vad vi säger och vad vi gör. Forskning visar att införandet av dataskyddsförordningen har haft en positiv inverkan på appars beteende och att de nu har mindre tillgång till data. Men det konstateras också att många appar fortfarande har åtkomst till fler funktioner än vad som beskrivs i integritetspolicyn och än vad de behöver för att fungera. Av undersökta Android-appar fanns det exempel på appar som registrerade användarens aktivitet och skickade informationen till olika servrar vilket, enligt forskarna, kan leda till digital övervakning, profilering och lösenordsfiske. Detta medför risker för den personliga integriteten.[318]

Ett pågående forskningsprojekt undersöker användarnas uppfattning om hur (fysisk) fingeravtrycksigenkänning fungerar och varför. Forskningen visar på skillnaden mellan att använda PIN-kod och fingeravtryck vid inloggning. Studien visar bland annat att självuppskattning av kunskap i datasäkerhet inte är en bra indikator för respondenters faktiska förståelse för hur säkra fingeravtryck är.[319]

315. S. Larsson (projektledare), *Tillitsbaserad personuppgiftshantering i den digitala ekonomin*. Lunds universitet, 2020.

316. Vinnova/RISE *Sjyst data!* – Slutrapport november 2019. Vinnova Utmaningsdriven Innovation (UDI), Steg 2.

317. H. Jonsson, *From Signal to Social: Steps Towards Pervasive Social Context*. Lunds universitet, 2018. Se artikel: https://www.forskning.se/2018/10/16/digitalt-fingeravtryck-hotar-din-integritet/.

318. L. Fritsch, M. Hatamian, N. Momen, artiklar: *Did App Privacy Improve After the GDPR?*, Karlstads universitet. 2019. *GDPR lyft för appar*, https://voister.se/artikel/2019/11/gdpr-lyft-for-appar/. Även *A Multilateral Privacy Impact Analysis Methos for Android Apps*, 2019. Ingår i: *Privacy Technologies and Policy/*[ed] M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina & A. Bourka, Cham: Springer, 2019, Vol. 11498, sid. 87-106.

319. F. Faregar, J.S. Pettersson, S. Fisher-Hübnern, *Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood*. Karlstad universitet, 2018.

7.1.3 Användning av appar inom AdTechsektorn

När vi rör oss i digitala miljöer, blir vi kontinuerligt följda och profilerade. För AdTechsektorn, är tillgång till data som vi lämnar i dessa miljöer av stor betydelse för att kunna rikta specialdesignad marknadsföring till enskilda.

Några av de risker som finns inom AdTechsektorn har tidigare beskrivits i avsnittet om teknikutveckling (avsnitt 5.4.3) . Där redovisas också norska Forbrukerrådets rapport som drar slutsatsen att appar samlar in stora mängder data och att AdTechsektorn delar och behandlar data helt ”out of control”.[320]

En studie på temat dataekonomier visar hur den digitala ekonomin under de senaste 25 åren har utvecklats mot ett alltmer datadrivet ekosystem, djupt involverat i de flesta aspekter av våra vardagsliv.[321]

Annonsfinansiering av riktad reklam tycks idag, enligt rapporten, vara en central affärsmodell för webben, vilket bidrar till insamling av stora mängder individrelaterad data. Studien visar på komplexiteten i reklamprocessen och konstaterar att de flesta webbplatsbesök medför att en stor mängd tredjeparter samlar in data och spårar besöket, om inte särskilda åtgärder tagits av besökaren för att förhindra detta.

Användare och konsumenter är enligt rapporten i varierande grad medvetna om datainsamlingen, Ofta finns ett grundläggande antagande om att ens data kommer användas för riktad reklam, men i övrigt finns låg grad av transparens vad gäller tredjepartsaktörer och vad datan används till. Medgivandet till datainsamling tycks ofta vara oinformerat, vilket indikerar att regleringen kring kakor och informerat samtycke inte fungerar. Tredjepartsproblematiken och datahandlande marknader utgör, både från ett individ- och ett företagsperspektiv , en icke-transparent praktik. Konsumenters informerade valfrihet är därigenom undergrävd.

En av slutsatserna i rapporten är att mycket talar för att dataekonomier och kommersiella plattformsaktörers dominans föranleder ett ökat samverkansbehov mellan tillsynsmyndigheter som IMY, Konsumentverket och Konkurrensverket och att dessa behöver säkerställa att de har erforderlig kompetens och effektiva tillsynsmetoder för att kunna granska aktörerna på AdTech-marknaden.

320. Forbrukerrådet *Out of control. How consumers are exploited by the online advertising industry*, 2020.

321. S. Larsson, på uppdrag av Konkurrensverket, uppdragsforskningsrapport 2020:4 *Dataekonomier – Om plattformar, tredjepartsaktörer och behovet av transparens på digitala marknader.* I rapporten framhålls att där tidigare i huvudsak konsumenträtt och integritetsfrågorna stått i fokus, har konkurrensfrågorna fått ett allt större fokus på området, i takt med att vissa av digitaliseringens datadrivna aktörer erhållit en nästan infrastrukturell marknadsposition.

7.1.4 Akademin utvecklar dataskyddsutbildningar

Kunskap om dataskyddsförordningen och hur förordningen påverkar den egna verksamheten är central för en effektiv implementering i verksamheterna. Utvecklare och designers saknar ofta kunskap om data- och integritetsskyddsfrågor och behöver stöttning i att göra rätt i designsituationer. Genom ett online-verktyg som utvecklats kan mjukvaruarkitekter och utvecklare få stöd i att ta fram system som är anpassade efter förordningen. Forskare vid Karlstads universitet har arbetat fram breda onlineutbildningar i dataskydd, bland annat en med särskilt inriktning mot Privacy by Design, för professionella och universitets- och högskolestudenter.[322] Totalt finns fem separata moduler i utbildningskonceptet,[323] som utöver stöd vid mjukvarudesign för utvecklare och designers, som nämnts ovan, omfattar

- **Introduktion** i integritetsskydd och GDPR[324] – utbildningen ger grundläggande kunskaper och diskuterar typiska risksituationer i samband med användning av molntjänster, IoT och Big Data. I utbildningen presenteras åtgärder som verksamheter måste vidta för att uppfylla dataskyddsförordningens krav.
- **Integritetshöjande tekniker** (Privacy Enhancing Technologies, PET) – ger en introduktion till säkerhets- och integritetshöjande mekanismer och tekniker.
- **Integritetsdesign** – introduktion till inbyggt dataskydd och dataskydd som standard och integritetsvänlig design. Utbildningen anger bland annat hur en konsekvensanalys kan genomföras.
- **Strategiskt dataskyddsarbete** (Privacy Management) – anger att ett strategiskt dataskyddsarbete är en kontinuerlig process för att bedöma risker och konsekvenser i verksamheten. Under utbildningen tillhandahålls bland annat en modul för strategiskt dataskyddsarbete som en del i verksamhetens organisatoriska åtgärder.

Det är vällovliga initiativ och utbildning kan bidra till en djupare förståelse av olika aspekter av integritet och informationssäkerhet i praktiken.

322. M. Colesky, K. Dementzou, L. Fritsch, S. Herold *Helping Software Architects Familiarize with the General Data Protection Regulation*, Karlstads universitet, 2019. D. Lynette, C. Marianthi Theocharidou, S. Fisher-Hübner, L. Martucci, L. Fritsch, T. Pulls *MOOC on Privacy by Design and the GDPR*.

323. S.Alfredsson, S. Fischer-Hübner, L. Fritsch, S. Herold, L. Iwaya, L. Martucci, T. Pulls, A. Zuccato *The Privacy by Design course team*, https://www.kau.se/en/cs/en/pbd.

324. Integritetsskyddslagstiftningen utgör också ett särskilt inslag i den obligatoriska kursen i rättsinformatik på juristprogrammet på Stockholms universitet.

7.1.5 Forskning för att utveckla säkra molntjänster och appar

Ett europeiskt forskningsprojekt bedrivs i syfte att skapa en ny plattform som möjliggör säker analys av data i molnet. Den nya tjänsten syftar till att kunna erbjuda en helt säker analys av känsliga data som till exempel patientuppgifter. Förutom att plattformen ska möjliggöra en säker analys av känsliga uppgifter, uppges den kunna ge stora värden genom att kunna se större mönster i stora datamängder utan att enskilda kan spåras. Exempelvis skulle större telefonoperatörer, som idag är strikt begränsade i vilken information de får använda och hur, kunna analysera rörelser generellt och därmed kunna kartlägga trender i rörelsemönster i samhället utan att enskilda kan identifieras. Forskningen omfattar även utveckling av ett verktyg som förklarar hur registrerades uppgifter analyseras säkert och integritetsvänligt.[325]

Ett annat forskningsprojekt anger att en central faktor för system som hanterar känslig information, till exempel medicinsk data, är att de är säkra. I den mån patienter inte har tillit till systemen kommer de inte att lämna nödvändiga uppgifter för att en läkare ska kunna göra en adekvat medicinsk bedömning. Trots det anges att många av dagens mobila lösningar för hälsodatainsamling saknar tillräckligt säkerhets- och integritetsskydd. Ett samverkansprojekt mellan svenska och brasilianska forskare har resulterat i framtagning av en säker och integritetsskyddande app för mobil insamling av hälsodata, där Privacy by Design och by Default är viktiga komponenter. Designen är anpassad för utvecklare med begränsade kunskaper i integritetsskyddande system, i syfte att de löpande ska kunna ansvara för att genomföra uppdateringar och underhåll av systemet.[326]

325. S. Fischer-Hübner *Säkrare användning av molntjänster med avidentifiering*, Karlstad universitet. Projektet avslutas 2022.

326. L. Horn Iwaya *Engineering Privacy for Mobile Health Data Collection Systems in the Primary Care*, Karlstad universitet, 2019.

7.1.6 Internet of things, IoT

Uppkopplade enheter i hemmet kan kontinuerligt samla in och föra vidare data om de boendes dagliga aktiviteter. Insamlingen kan omfatta mycket integritetskänslig data. I ett pågående forskningsprojekt beskrivs i problemformuleringen att en del av uppgifterna tillhandahålls frivilligt av användarna, medan andra data samlas in automatiskt av enheterna. I vissa fall kan slutanvändare inte (enkelt) välja bort insamlingen av data och många gånger ”begravs” samtycken för insamling eller användning av data i integritetspolicyn och accepteras omedvetet av användarna. Om en användare upphör med att tillhandahålla informationen upphör tjänsterna ibland att gälla. Genom att identifiera och kartlägga de hot och integritetsrisker som finns i system för uppkopplade enheter i hemmet, kan nya system byggas som skyddar den personliga integriteten. Forskningen syftar till att höja integritetsskyddet och ge individerna större kontroll över de uppkopplade enheterna.[327]

Ytterligare ett forskningsprojekt inom IoT bedrivs i syfte att studera effekterna av sensorbaserad teknologi. Inom forskningen studeras användning av sensorbaserad teknik inom områden som tidigare varit huvudsakligen analoga eller som använt sig av digital teknik som inte varit sensorbaserad. Sensorbaserad teknik och digital databehandlingsförmåga används allt oftare och blir allt mer kraftfull. Det finns därför ett behov av att undersöka etiska aspekter och sociala implikationer. Genom att belysa detta i samband med strategier för implementering avser projektet att skapa en brygga mellan det praktiska och det akademiska och därigenom generera ett värde för såväl akademi som praktiker när det kommer till förståelsen för IoT.[328]

Ett av problemen med smarta enheter är att det går att spåra personer och kartlägga deras aktiviteter. Ofta behöver man lämna uppgifter som inte borde vara av relevans för att få produkten att fungera. Ett forskningsprojekt arbetar nu för att kartlägga problemen i syfte att höja säkerheten för nästa generations smarta enheter och miljöer. Projektet syftar till att höja säkerheten för användarna med hjälp av den senaste tekniken i identitetshanteringen. Användaren ska få större kontroll genom att till exempel ha möjlighet att interagera i ett sekretessvänligt läge. Projektet ska resultera i en prototyp för olika komponenter som kan säkra den personliga integriteten som medför pålitliga smarta miljöer som ger människor kontroll och överblick över sina enheter.[329]

327. J Bugeja, *Smart connected homes: concepts, risks and challenges*. Lic.avh Malmö universitet. Forskningen påbörjad 2018.

328. V. Mähler *Värdeskapande med internet of things*. Umeå universiet. Forskningsprojektet avses avslutas i oktober 2021.

329. Projekt SURPRISE *Secure and Private Connectivity in Smart Environment*, Karlstads universitet. Projektet startade 2019 och ska pågå i fem år.

7.1.7 Artificiell intelligens, AI

Just nu är det akademiska intresset för AI stort och utveckling och forskning bedrivs på flera orter i Sverige, och utomlands. Vinnova uppskattade 2019 antalet forskningsmiljöer i Sverige som fokuserar på AI då till närmare 40, men framhöll samtidigt att det är ett snabbt växande område.[330] 2019 startade, som nämnts tidigare, ett nationell samverkanscentrum benämnt AI Sweden som genom samverkan och samlokalisering ska accelerera innovation och forskning inom praktiskt tillämpad AI. Vinnova är en av huvudfinansiärerna. Syftet är att kraftsamla kring forskning och innovation inom AI. Sannolikt kommer vi inom de kommande åren att se flera resultat av detta samarbete.[331]

Den snabba utvecklingen inom AI innebär utmaningar för integriteten, vilket kan skada tilliten till tekniken. I en nyligen publicerad rapport presenterar fyra forskare såväl problemområden som förslag till lösningar. Att AI och den snabba utvecklingen inom maskininlärning kommer med enorma löften är idag vedertaget. Men om dess värden kommer att kunna realiseras på ett hållbart sätt är enligt forskarna mer osäkert. Det beror bland annat på att etiska, sociala och rättsliga dimensioner inte har integrerats och testats tillräckligt i forskning, utformning och implementering av AI-systemen. Detta riskerar att leda till mindre tillförlitliga AI-applikationer och skada tilliten till AI överlag.[332]

De fyra problemområden som forskarna identifierar som nyckelområden för AI-teknologins fortsatta framgångsrika utveckling är:

- partiskhet/”bias”
- ansvarsfrågor
- missbruk och illvillig användning samt
- transparens och förklarbarhet.

Forskningsrapportens rekommendationer är att *regleringen behöver förtydligas*; såväl etiska ramverk som tolkning av rådande lagstiftning behöver stärkas och tillsynsmyndigheterna behöver stimuleras och utbildas för att kunna hålla jämna steg med utvecklingen. Man behöver också satsa på *tvärvetenskapliga perspektiv* (dels forskningsmässigt, till exempel inom teknik- och samhällsvetenskap, samt medicin och humaniora, dels samarbetsmässigt, där samarbeten behöver etableras mellan akademi, industri och offentlig sektor) kring tillämpad AI för att nå mer kunskaper om utmaningarna, bland annat när det gäller bias, ansvarsfördelning och vilken grad av transparens som är önskvärd/möjlig för respektive kontext eller användning. Slutligen behöver *tilliten i samhället för AI stärkas*. Tillitsfrågan är central om de löften och värden AI kan medföra i sektorer som handel (individualisering), finans (effektivisering) och hälso- och sjukvård (ökad precision i diagnoser) ska kunna realiseras.

Ytterligare en forskningsartikel beskriver vad AI kan användas till, men tar också upp legala och normativa risker och diskuterar olika förutsättningar för att tillit till systemet och utvecklingen ska finnas.[333]

Också Sveriges konsumenter har gjort en undersökning om AI där de konstaterar att den stora frågan inte är om vi är för eller emot AI, utan om hur vi gemensamt kan skapa AI-system som både konsumenter, företag och myndigheter kan lita på.[334]

Några av de utmaningar som enligt Sveriges Konsumenter finns med AI anges vara bristen på transparens, vilket kan bero på allt från att företag inte vill dela med sig av affärshemligheter, till att systemen utgör ”svarta lådor” vars logiska slutsatser är obegripliga för människor. Sveriges konsumenter menar att transparens är en förutsättning för att kunna avgöra om ett system fyller sin funktion och gör det på ett rättvisande sätt. Både konsumenter och tillsynsmyndigheter måste ges insyn i de system som rullas ut och där systemen sköter beslutsfattande i allt viktigare frågor. Konsumenter bör under alla omständigheter få kunskap om att automatiserat beslutsfattande används och vilka data besluten baseras på.[335] I de fall beslutet kan innebära ekonomiska eller andra allvarliga konsekvenser bör de kunna få en mer utförlig förklaring av systemets beslut.

330. Vinnova rapport VR 2019:05 *AI-miljöer i Sverige – En översikt över miljöer som bidrar till utvecklingen av artificiell intelligens*. I rapporten anges att översikten inte är fullständig på grund av den snabba förändringstakten inom området.

331. https://www.vinnova.se/m/artificiell-intelligens-ai/

332. S. Larsson, F. Heintz, L. Felländer-Tsai, A. Felländer *AI-teknologin måste gå att lita på*, Lunds universitet, 2019.

333. S. Larsson *The Socio-Legal Relevance of Artificial Intelligence*, Lunds universitet, 2019.

334. Sveriges konsumenters rapport *AI, Artificiell intelligens. Konsumentskydd för transparens & tillit*, 2020.

335. Dataskyddsförordningen innehåller särskilda bestämmelser om automatiserat beslutsfattande i artikel 15.1 h och artikel 22.

Tre områden som särskilt lyfts fram som riskområden för diskriminering och osaklig särbehandling inom AI enligt Sveriges Konsumenter rör personanpassade försäkringspremier inom försäkringsbranschen och personanpassade priser i övrigt, som sannolikt förekommer i allt högre utsträckning, där prisanpassningar baseras på om en konsument till exempel är innehavare av en hemsida eller app eller var de befinner sig när de handlar. Därutöver är ett riskområde annonsmarknaden där reklam och jobbannonser riktas till specifika målgrupper.

System för personanpassad marknadsföring är inte isolerade till sociala medier utan används över hela webben. I många fall riktar annonsörer (eller väljer att inte rikta) budskap baserat på känsliga personuppgifter, som trosuppfattning och sexuell läggning. Systemen inkluderar dessutom ofta många typer av uppgifter, till exempel om köphistorik, inkomst, geografisk plats och personlighetsdrag. Kunskapen kan sedan användas för att rikta reklam. Enligt Sveriges konsumenters rapport hävdas att man inom Adtech-sektorn utlovar att man kan skräddarsy reklam så att man når fram med sina budskap vid specifika tidpunkter då konsumenter är särskilt mottagliga för reklambudskap.[336]

Ett riskområde som utvecklare av AI-system uppmanas undvika eller kompensera för enligt Sveriges konsumenter rör endimensionella mål. Trots fokus på intelligens och automatisering följer AI-system i grunden instruktioner som är upp till människor att definiera. Är incitamenten felaktiga, och till exempel enbart utgår från att optimera vinst, kan det snedvrida inlärningen. Bristfälliga data under upplärningen utgör ytterligare ett riskområde. Om människor tidigare har diskriminerat konsumenter baserat på exempelvis kön eller etnisk bakgrund är risken stor att AI-systemet lär sig samma beteende. Proxyegenskaper är ett tredjeriskområde. Egenskaper kön, etnicitet och sexuell läggning korrelerar ofta med andra uppgifter om en person; etnicitet kan till exempel korrelera med postnummer, medan kön kan korrelera med inköp av vissa produkter. AI-systemet kan därmed programmeras på ett sätt som leder till diskriminering.

336. Direktmarknadsföring anses vara en fråga som medborgare bör ha särskild förfoganderätt över och det finns särskilda bestämmelser om att man ska ha rätt att tacka nej till direktreklam (rätten att göra invändningar, artikel 21.2 dataskyddsförordningen). För de verksamheter som bygger sin verksamhet på samtycken från enskilda är det här viktigt att arbeta med transparens och utifrån förutsättningen att enskilda alltid har rätt att när som helst återkalla samtycket. Dennes personuppgifter får då inte längre behandlas (artikel 6.1 (a), samt artikel 7–8 dataskyddsförordningen).

7.1.8 Sammanfattning

Sammanfattningsvis kan konstateras att pågående forskning och studier pekar på områden där särskilda integritetsrisker finns och antingen bidrar till att öka förståelsen för området och de risker som finns, eller bidrar med förslag på lösningar för att integritetsskyddet ska beaktas i utvecklingen av olika tjänster och produkter. Områden där särskilda risker analyseras är appar och dess tillämpning, särskilt annonsfinansierade appar, där undersökningar särskilt pekar på den omfattande spridning av uppgifter som apparna bidrar till och svårigheterna för enskilda att ge ett informerat samtycke till tjänsten. Det är också uppenbart att appar bidrar till att enskilda förhållandevis enkelt kan identifieras och övervakas.

Särskilda risker för en omfattande datainsamling och för övervakning och kartläggning av enskilda lyfts fram när det gäller utvecklingen av IoT. Detsamma gäller för den snabba utvecklingen som idag sker inom AI, där särskilda risker finns för att AI utvecklas utifrån förutsättningar som riskerar att leda till diskriminering eller på annat sätt oönskade resultat. Ett särskilt riskområde är här kopplat till automatiskt beslutsfattande.

Bilaga 1 – sammanfattning av centrala regler i dataskyddsförordningen

I denna bilaga beskrivs några av de förändringar som har införts genom dataskyddsreformen och som kortfattat har berörts i rapporten.

Enskildas rättigheter har stärkts

Enskildas rättigheter har stärkts genom införandet av förordningen. I avsnitt 3 och 4 i förordningen behandlas de rättigheter som verksamheter måste tillförsäkra enskilda vid behandling av deras uppgifter.[337] Det handlar om att enskilda ska ha rätt till insyn och kontroll över sina personuppgifter genom att få

rätt till information och tillgång

- klar och tydlig information, samt klara och tydliga villkor för hur man som enskild ska kunna utöva sina rättigheter – den enskilde ska få relevant information i klar och tydlig, begriplig och lättillgänglig form
- viss information om uppgifter har samlats in från den enskilde själv, annan information om uppgifter har samlats in från annan; ändamålen med behandlingen och den rättsliga grunden ska alltid anges
- information om och bekräftelse på om personuppgifter om en själv behandlas

rätt till rättelse, radering, begränsning och överföring

- rätt att få uppgifter rättade
- rätt att få uppgifter raderade (rätten att bli bortglömd)
- rätt att begränsa behandlingen
- rätt till så kallad dataportabilitet, det vill säga att få ut de personuppgifter som rör en själv för att kunna föra över dem till en annan aktör

rätt att göra invändningar

- rätt att göra invändningar om personuppgifter behandlas med stöd av en intresseavvägning eller ett allmänt intresse (inklusive profilering) – personuppgifterna får då inte längre behandlas om inte personuppgiftsansvarige kan påvisa avgörande berättigande skäl som väger tyngre än den enskildes intressen, för att fortsätta behandlingen
- rätt att invända om personuppgifter behandlas för direktmarknadsföring, inklusive mot profilering i den utsträckning profileringen har samband med direktmarknadsföring

begränsning av automatiserade beslut

- rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som har rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.

Dataskyddsförordningen anger rättigheter för enskilda som ska gälla i alla medlemsstater, bland annat ska enskilda, utöver de rättigheter som särskilt pekas ut, ha rätt att lämna in klagomål till tillsynsmyndigheten. De ska också ha möjlighet att kunna klaga på beslut från dataskyddsmyndigheten, processa mot en personuppgiftsansvarig i nationell domstol och ha rätt till skadestånd för skada som uppstått genom överträdelser av dataskyddsförordningen.[338]

Den enskildes rättigheter är långtgående och förutsätter att den som hanterar personuppgifter har ordning och reda och kan härleda personuppgifter som kan kopplas till en viss individ samt också rutiner och processer för att ge enskilda den insyn och kontroll över sina uppgifter de har rätt till.

337. Artikel 12–22 dataskyddsförordningen.

338. Artikel 77–82. Rätten till skadestånd behandlas bland annat i avhandlingen *Integritet och skadestånd. Om skyddet för personuppgifter och privatliv i svensk rätt*; Ak. avh. 2020, Uppsala universitet.

Kraven på verksamheter som behandlar personuppgifter har ökat

Som huvudregel är det den som hanterar enskildas uppgifter som har att visa att den enskildes rättigheter är tillgodosedda vid en eventuell granskning.

Begreppen behandling och personuppgift är centrala i regelverket

När en verksamhet behandlar personuppgifter aktiveras ett stort ansvar och en rad skyldigheter.[339] Begreppet behandling definieras i dataskyddsförordningen. IMY har i vägledning till företag, myndigheter och andra organisationer definierat begreppet personuppgiftsbehandling genom att exemplifiera en serie av åtgärder som behandlingen kan innebära.[340] En behandling av personuppgifter är varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring

Med personuppgift avses en uppgift som direkt eller indirekt identifierar en fysisk person, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Genom den stora omfattningen av potentiella identifierare är det tydligt att behandling av personuppgifter omfattar en stor mängd ageranden.[341]

339. Artikel 4 (2) dataskyddsförordningen.

340. Den fullständiga definitionen av *behandling* framgår av artikel 4 (2) i dataskyddsförordningen: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. Definitionen av *personuppgifter* framgår av artikel 4 (1): varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

341. Artikel 4 (1) dataskyddsförordningen.

Grundläggande principer behöver beaktas vid all hantering av personuppgifter

Förordningen ställer ökade krav på den som behandlar personuppgifter. Kraven på en personuppgiftsansvarig är bland annat att man vid behandling av personuppgifter följer de grundläggande principerna:[342]

laglighet, korrekthet och öppenhet – uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade

ändamålsbegränsning – uppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (den så kallade finalitetsprincipen)[343]

uppgiftsminimering – uppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas

korrekthet – uppgifter ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål

lagringsminimering[344] – uppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.[345]

integritet och konfidentialitet – uppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet – inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse – med användning av lämpliga tekniska eller organisatoriska åtgärder.

Därutöver anges principen om ansvarsskyldighet – den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna efterlevs.

342. Artikel 5.1 (a–f) dataskyddsförordningen.

343. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i förordningen anses inte vara oförenlig med de ursprungliga ändamålen.

344. Principen om lagringsminimering gäller inte för bestämmelser som anger att uppgifter ska sparas under vissa perioder i annan lagstiftning. Exempelvis finns krav inom offentlig verksamhet på att uppgifter ska sparas om det inte finns gallringsföreskrifter som medger att uppgifter får gallras. Det finns också föreskrifter exempelvis i bokföringslagen om hur länge bokföringsmaterial måste bevaras i bokföringssyfte.

345. Personuppgifter får lagras under längre perioder om de enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i förordningen, under förutsättning att lämpliga tekniska och organisatoriska åtgärder genomförs för att säkerställa den registrerades rättigheter och friheter.

Rättsliga grunder som gör behandling av personuppgifter tillåten

En vanlig fråga och vanliga klagomål rör den rättsliga grunden för att någon ska få hantera personuppgifter. Enligt förordningen finns sex rättsliga grunder som gör att personuppgiftsbehandlingen kan uppfylla den grundläggande principen om legalitet. För den personuppgiftsansvarige betyder det att denna har att säkerställa att den personuppgiftsbehandling som genomförs har stöd i någon av de rättsliga grunderna. De rättsliga grunderna som kan utgöra rättsligt stöd för behandlingen är

samtycke – den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål. Samtycket ska vara frivilligt och uttryckligt och ska när som helst kunna återkallas. Personuppgifterna får då inte längre behandlas. Samtycke kan sällan användas av offentliga aktörer eller i andra sammanhang där det råder en obalans i maktförhållandet mellan den enskilde och den andra parten, till exempel vid anställningsförhållanden

avtal – behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås

rättslig förpliktelse – behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige

vitalt intresse – behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person

allmänt intresse – behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Grunden gäller framför allt i offentlig verksamhet men används även när privata aktörer utför en uppgift av allmänt intresse

intresseavvägning – behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn. Intresseavvägning kan inte användas av myndigheter.

Grunderna kopplar som nämnts till den grundläggande principen om laglighet – uppfyller man inte någon av dem är den tilltänkta eller önskade behandlingen av personuppgifter inte tillåten.

Krav på tillräckliga säkerhetsåtgärder för att skydda personuppgifterna

Dataskyddsreglerna innehåller också flera bestämmelser om säkerhetsåtgärder. Den utökade användningen av stora mängder personuppgifter har ökat kraven på adekvat skydd för dessa. Regelverket adresserar frågan på flera sätt.

Skyddet för den personliga integriteten är en grundläggande princip – ansvar för integritet och konfidentialitet – och krav på tillräcklig säkerhet – hör, som har beskrivits, till en av de grundläggande principerna i dataskyddsförordningen.[346] Utgångspunkten är att den personuppgiftsansvarige måste säkerställa att åtgärder vidtas som leder till att uppgifterna ges tillräckligt skydd mot obehörig eller otillåten behandling, förlust, förstöring eller skada.

Den personuppgiftsansvarige har ett utpekat ansvar att genomföra ett strategiskt och systematiskt arbete kring hur personuppgifter får hanteras – den personuppgiftsansvarige har ett utpekat ansvar för hur personuppgifter hanteras i verksamheten. Det handlar som nämnts om att anpassa verksamheten så att de grundläggande principerna uppfylls och det finns stöd i en rättslig grund. Detta förutsätter i grunden ett löpande och systematiskt arbete med att säkerställa att de personuppgifter som hanteras i verksamheten löpande har tillräckligt skydd och att man har kontroll över vilka uppgifter som hanteras i verksamheten, varför, på vilket sätt och av vem.

Förordningen pekar på flera sätt ut ansvaret för den personuppgiftsansvarige. Flera bestämmelser pekar på vikten av att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen.[347] Det är inte frågan om att detta ska göras vid ett enstaka tillfälle utan ansvarig har att se över och uppdatera åtgärderna vid behov.

346. Artikel 5.1 (f) dataskyddsförordningen.

347. Utöver artikel 5.2 (ansvarsskyldigheten), artikel 24 dataskyddsförordningen.

Det finns krav på att bygga in dataskydd i de tekniska och organisatoriska åtgärder som implementeras, till exempel pseudonymisering (inbyggt dataskydd), men också säkerställa att inställningar anpassas och åtgärder vidtas för att tillgodose de grundläggande principerna, exempelvis uppgiftsminimering (dataskydd som standard). Framför allt ska åtgärderna säkerställa att personuppgifter inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.[348] Åtgärder behöver övervägas både vid fastställandet av hur behandlingen ska utföras och vid själva behandlingen.

Hur omfattande åtgärder som behöver vidtas är beroende av dels den tekniska utvecklingen, vad som är möjligt och hur mycket det skulle kosta att genomföra åtgärderna, dels behandlingens art, omfattning, sammanhang och ändamål samt vilka risker den medför för enskilda.

Utgångspunkten är således att personuppgiftsansvariga har omfattande krav på sig när de behandlar personuppgifter att löpande vidta åtgärder för att säkerställa att personuppgifter ges ett tillräckligt skydd mot obehörig eller otillåten behandling, förlust, förstöring eller skada.

Säkerheten måste löpande säkerställas i samband med att behandling sker – det finns ytterligare bestämmelser som pekar ut hur säkerheten ska säkerställas.[349] Den personuppgiftsansvarige har att vidta tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Åtgärderna kan, när det är lämpligt, omfatta till exempel

- pseudonymisering och kryptering av personuppgifter
- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystem och tjänster
- förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet för oavsiktlig eller olaglig förstöring, förlust eller ändring eller för obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Den personuppgiftsansvarige ska vidta åtgärder för att säkerställa att varje person som utför arbete under dennes överinseende och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige.

Krav på konsekvensbedömning som ett led i att värdera risker – den personuppgiftsansvarige ska, som har framgått, löpande bedöma de risker som uppstår genom att personuppgifter behandlas i verksamheten. Ett stöd för att göra detta är att göra riskanalyser. I dataskyddsförordningen ställs krav på en särskild typ av riskbedömning som kallas konsekvensbedömning[350]. En sådan ska genomföras om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en *hög risk* för fysiska personers rättigheter och friheter. I sådana fall ska en konsekvensbedömning göras *innan* personuppgifter börjar behandlas.

För brottsbekämpande myndigheter är kraven på konsekvensbedömning högre. En sådan ska genomföras om en ny typ av behandling, eller betydande förändringar av redan pågående behandling, kan antas medföra *särskild risk* för intrång i den registrerades personliga integritet.[351]

348. Artikel 25 dataskyddsförordningen.
349. Artikel 32 dataskyddsförordningen.
350. Konsekvensbedömning i samband med lagstiftning behandlas i avsnitt 6.3.1.2
351. 3 kap. 7 § första stycket brottsdatalagen.

Särskilt om kraven på konsekvensbedömning

En konsekvensbedömning ska i vart fall innehålla

- en systematisk beskrivning av den planerade behandlingen och behandlingens syften
- en bedömning av behovet och, när så är lämpligt, den personuppgiftsansvariges berättigade intresse av behandlingen
- en bedömning av riskerna för de registrerades rättigheter och friheter
- de åtgärder som planeras för att hantera riskerna (exempelvis skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna) och för att visa att förordningen efterlevs
- en bedömning och analys av proportionaliteten hos behandlingen i förhållande till syftena.

En konsekvensbedömning behövs särskilt när det är frågan om

- en systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling (inbegripet profilering) och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller i betydande grad påverkar fysiska personer
- behandling i stor omfattning av känsliga personuppgifter, personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott
- systematisk övervakning av en allmän plats i stor omfattning.

IMY har tagit fram en förteckning där mer konkreta exempel ges på när en konsekvensbedömning behöver genomföras.[352]

Krav på konsekvensbedömning föreligger om den planerade behandlingen uppfyller minst två av följande kriterier; behandlingen

1. *utvärderar eller poängsätter* människor; till exempel genetiska tester som erbjuds konsumenter för att bedöma och förutse risker för sjukdomar, eller kreditupplysningsföretag eller företag som profilerar internetanvändare
2. sker i syfte att fatta *automatiserade beslut* som har rättsliga eller betydande följder för den registrerade
3. *medför systematisk övervakning av människor*, till exempel genom kameraövervakning av en allmän plats eller genom insamling av uppgifter från internetanvändning i offentliga miljöer
4. *avser känsliga personuppgifter* eller uppgifter som är av mycket personlig karaktär, till exempel sjukhus som lagrar patientjournaler, företag som samlar in lokaliseringsuppgifter eller banker som hanterar finansiella uppgifter
5. sker i *stor omfattning*
6. kombinerar personuppgifter från olika behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, till exempel när man *samkör register*
7. avser personer som av något skäl befinner sig i ett *underläge eller i beroendeställning* och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter
8. avser *ny teknik eller nya organisatoriska lösningar*, till exempel en IoT-applikation
9. syftar till att *hindra registrerade från att få tillgång* till en tjänst eller ingå ett avtal, till exempel en banks granskning av kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.

När det gäller användning av ny teknik, eller användning av digitala plattformar eller tjänster som vanligen bygger på stora datamängder kan konstateras att en konsekvensbedömning ofta krävs.

352. Artikel 35.4 dataskyddsförordningen, https://www.datainspektionen.se/globalassets/dokument/beslut/forteckning---konsekvensbedomningar.pdf.

Exempel på behandlingar som kan kräva konsekvensbedömning är behandling av personuppgifter i samband med:

- tillhandahållande av sociala medieplattformar eller av smarta hem-produkter där insamling sker av detaljerade uppgifter om användningen av tjänsten
- installation av smarta elmätare hos elabonnenter för att kunna ta fram, överföra och analysera uppgifter som rör konsumenter på en detaljerad nivå
- system för intelligent videoanalys för att skilja ut bilar och automatiskt känna igen registreringsskyltar i syfte att övervaka körbeteendet på motorvägar, eller användning av kamerabevakning för att skilja ut registreringsnummer i syfte att debitera parkeringsavgifter
- insamling av bland annat lokaliseringsuppgifter i syfte att använda dessa vid exempelvis stads- och trafikplanering eller som uppkommer genom användning av smarta bilar, till exempel för att utveckla tekniken
- användning av välfärdsteknik, till exempel robotar eller kamerabevakning, i människors boenden
- myndigheters service genom digitala plattformar som leder till storskalig behandling av personuppgifter
- större förändringar i den tekniska infrastrukturen exempelvis inom hälso- och sjukvård eller social omsorg.

Andra exempel på behandlingar som kan kräva konsekvensbedömning rör följande.

- banker eller andra kreditinstitut som fattar automatiserade beslut om en kredit ska beviljas eller inte
- omfattande behandling av ekonomiska uppgifter för att kunna lämna ut dessa till andra aktörer för kreditupplysningsändamål
- omfattande behandling av uppgifter om kunders tidigare misskötsamhet (en s.k. svart lista) i syfte att avgöra om personen ska få återkomma som kund eller inte
- behandling av barns personuppgifter i skolverksamhet eller i social omsorg, om det är ett större antal registrerade.

En konsekvensbedömning kan vara nödvändig för att komma fram till vilka risker en tänkt behandling medför och för att kunna vidta relevanta åtgärder för att minska dessa risker.

Det bör återigen påpekas att en konsekvensbedömning ska genomföras om en behandling sannolikt leder till en *hög risk* för fysiska personers rättigheter och friheter. Om den personuppgiftsansvarige gör bedömningen att behandlingen sannolikt *inte* leder till en hög risk, finns således inte krav på att genomföra en konsekvensbedömning. I sådana fall bör dock den personuppgiftsansvarige *motivera och dokumentera* anledningarna till att en konsekvensbedömning inte utförs och inkludera ett ev. dataskyddsombuds synpunkter.

Även här ställs krav på uppföljning och den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen. Det ska i vart fall genomföras när den risk som behandlingen medför förändras.

Det kan sammanfattningsvis konstateras att kraven på konsekvensbedömning är höga och träffar stora delar av de nya tekniker, appar och systembyten som sker i teknikutvecklingen. Även om förhandssamråd inte behövs, fordras i många fall att en konsekvensbedömning har gjorts där dessa ställningstaganden framgår. Det är den personuppgiftsansvarige som har krav på sig att kunna visa att så har skett.

Krav på förhandssamråd

Om en konsekvensbedömning visar att en planerad behandling skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken, har den personuppgiftsansvarige att vidta åtgärder för att minska risken. Skulle behandlingen, trots vidtagna åtgärder, fortfarande medföra en hög risk för de registrerades grundläggande fri- och rättigheter ska den personuppgiftsansvarige begära förhandssamråd med tillsynsmyndigheten. Förhandssamrådet ska genomföras innan behandlingen påbörjas.[353]

Om tillsynsmyndigheten anser att den planerade behandlingen skulle strida mot förordningen, och särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, ska tillsynsmyndigheten ge den personuppgiftsansvarige (och i tillämpliga fall ett personuppgiftsbiträde) skriftliga råd. Tillsynsmyndigheten får i förhandssamrådsförfarandet utnyttja alla utredningsbefogenheter som myndigheten har tillgång till enligt förordningen.[354]

För brottsbekämpande myndigheter är kraven på förhandssamråd högre. Om konsekvensbedömningen visar att det finns särskild risk för intrång i registrerades personliga integritet eller om typen av behandling innebär särskild risk för intrång, ska den personuppgiftsansvarige begära förhandssamråd med tillsynsmyndigheten i god tid innan behandlingen påbörjas eller betydande förändringar genomförs. Perioden är här sex veckor med möjlighet till förlängning ytterligare sex veckor.

Krav på hantering av personuppgiftsincidenter

Det finns omfattande krav på skyndsam hantering om en personuppgiftsincident inträffar. En incident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.[355]

Vid en personuppgiftsincident ska den personuppgiftsansvarige skyndsamt och senast inom 72 timmar efter att ha fått vetskap om incidenten, anmäla den till tillsynsmyndigheten.[356] Incidenter behöver inte anmälas om det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om anmälan görs efter 72 timmar ska förseningen motiveras. Det finns även bestämmelser om personuppgiftsbiträdens ansvar för att underrätta den personuppgiftsansvarige. Det finns också krav på den personuppgiftsansvarige att dokumentera alla personuppgiftsincidenter på ett sätt som gör det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av bestämmelsen om incidentrapportering.

Det finns även en informationsplikt kopplad till incidenthanteringen. Om incidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

Information behövs inte om den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder som tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten (exempelvis om uppgifterna gjorts oläsbara för obehöriga, till exempel genom kryptering, ytterligare åtgärder har vidtagits som säkerställer att den höga risken för registrerades rättigheter och friheter sannolikt inte längre kommer att uppstå eller om informationsplikten skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

353. Artikel 36 dataskyddsförordningen.
354. Artikel 58 dataskyddsförordningen.
355. Artikel 4.12 dataskyddsförordningen.
356. Artikel 33 dataskyddsförordningen.

Integritetsskydds
myndigheten

Detta är Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten arbetar för att skydda medborgarnas alla personuppgifter, till exempel om hälsa och ekonomi, så att de hanteras korrekt och inte hamnar i orätta händer. Det är vi som granskar att företag, myndigheter och andra aktörer följer GDPR – dataskyddsförordningen. Vi utbildar och vägleder dem som behandlar personuppgifter. Vi påverkar även lagstiftningen. Vi vill se en hållbar och integritetsvänlig digitalisering. Vi är övertygade om att det går att värna medborgarnas trygghet och samhällets säkerhet, utan omotiverad kartläggning och övervakning. Tillsammans med övriga dataskyddsmyndigheter i EU arbetar vi för att medborgarnas personuppgifter ska ha samma skydd i hela unionen. Vi arbetar även för att kreditupplysning och inkassoverksamhet ska bedrivas på ett korrekt sätt. Vår vision är ett tryggt informationssamhälle, där vi tillsammans värnar den personliga integriteten.

Kontakta Integritetsskyddsmyndigheten

E-post: imy@imy.se
Webb: www.imy.se
Tel: 08-657 61 00.
Postadress: Integritetsskyddsmyndigheten,
Box 8114, 104 20 Stockholm.